
Article:
Tamaki, Kiyoshi, Curty, Marcos and Lucamarini, Marco orcid.org/0000-0002-7351-4622 (2016) Decoy-state quantum key distribution with a leaky source. New Journal of Physics. 065008. ISSN 1367-2630

https://doi.org/10.1088/1367-2630/18/6/065008

PAPER • OPEN ACCESS

Decoy-state quantum key distribution with a leaky source

New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

OPEN ACCESS

RECEIVED
23 December 2015

REVISED
20 May 2016

ACCEPTED FOR PUBLICATION
31 May 2016

PUBLISHED
20 June 2016

PAPER

Decoy-state quantum key distribution with a leaky source

Kiyoshi Tamaki[1,5], **Marcos Curty**[2,5] **and Marco Lucamarini**[3,4,5]

[1] NTT Basic Research Laboratories, NTT Corporation, 3-1, Morinosato-Wakamiya Atsugi-Shi, 243-0198, Japan
[2] EI Telecomunicación, Department of Signal Theory and Communications, University of Vigo, Vigo E-36310, Spain
[3] Toshiba Research Europe Ltd, 208 Cambridge Science Park, Cambridge CB4 0GZ, UK
[4] Toshiba Corporate Research & Development Center, 1 Komukai-Toshiba-Cho, Saiwai-ku, Kawasaki 212-8582, Japan
[5] All authors contributed equally to this work.

E-mail: mcurty@com.uvigo.es

Keywords: quantum key distribution, device-independent quantum key distribution, quantum communication, security analysis, information leakage, Trojan horse attacks

Abstract

In recent years, there has been a great effort to prove the security of quantum key distribution (QKD) with a minimum number of assumptions. Besides its intrinsic theoretical interest, this would allow for larger tolerance against device imperfections in the actual implementations. However, even in this device-independent scenario, one assumption seems unavoidable, that is, the presence of a protected space devoid of any unwanted information leakage in which the legitimate parties can privately generate, process and store their classical data. In this paper we relax this unrealistic and hardly feasible assumption and introduce a general formalism to tackle the information leakage problem in most of existing QKD systems. More specifically, we prove the security of optical QKD systems using phase and intensity modulators in their transmitters, which leak the setting information in an arbitrary manner. We apply our security proof to cases of practical interest and show key rates similar to those obtained in a perfectly shielded environment. Our work constitutes a fundamental step forward in guaranteeing implementation security of quantum communication systems.

1. Introduction

It is well-known that two spatially separated users (Alice and Bob) can secretly communicate over a public channel if they own two identical random keys unknown to any third party. They can use their keys to enable symmetric-key encryption. When the symmetric-key algorithm is the so-called 'one-time pad' [1], the security of the resulting communication is independent of the computational capability of an eavesdropper (Eve) [2]. The only provably secure way known to date to distill secret random keys at remote locations is quantum key distribution (QKD) [3–6]. While the theoretical security of QKD has been convincingly proven in recent years [5], in practice a QKD realisation cannot typically perfectly satisfy the requirements imposed by the theory. Therefore it is crucial that security proofs are extended to accommodate the imperfections of the real QKD devices. Any unaccounted imperfection constitutes a so-called 'side-channel', which can be exploited by Eve to compromise the security of the system [7–17].

To close the gap between theory and practice, various approaches have been proposed so far, with two most prominent examples being 'device-independent QKD' [18–21] and decoy-state 'measurement-device-independent QKD' (mdiQKD) [22]. Device-independent QKD does not require a complete knowledge of how QKD apparatuses operate, being its security based on the violation of a Bell inequality. However, its experimental complexity is unsuitable for practical applications, as its ultimate form demands that Alice and Bob perform a loophole-free Bell test [23–25] in every QKD session. Also, its secret key rate is very poor with current technology [26, 27]. Decoy-state mdiQKD, on the other hand, permits to remove any assumption of trustfulness from the measurement device, which is arguably the weakest part of QKD realisations [7–14]. Under the only additional requirement that Alice and Bob know their state preparation process [28], mdiQKD with decoy-states allows to bring QKD theory closer to practice [29] without frustrating the key rate [22, 30]. Most

importantly, its practical feasibility has been already experimentally demonstrated both in laboratories and in field trials [31–38], with a key rate comparable to that of standard QKD protocols [37].

However, it is important to notice that the security of any form of QKD, including the two solutions above, relies on the assumption that Alice and Bob's devices do not leak any unwanted information to the outside. That is, their apparatuses must be inside private spaces that are well-shielded and inaccessible to Eve (see, e.g., [39]). This assumption is very hard, if not impossible, to guarantee in practice. The behaviour of real devices is affected by the environmental conditions and can depend on their response to external signals, unawarely triggered by a legitimate user, or maliciously injected into the QKD system by Eve. This could open new side-channels, of which the so-called Trojan-horse attack (THA) [40–42] is a meaningful example. While mdiQKD relieves QKD from the burden of characterising the measuring devices, the THA deals with the important question of guaranteeing a protected boundary between the transmitting devices, assigned with the preparation of the initial quantum states, and the outside world.

In a THA, Eve injects bright light pulses into the users' devices and analyse the back-reflected light, with the aim of extracting more information from the signals travelling in the quantum channel. Recently, [42] considered a feasible THA targeting the phase modulator (PM) of a QKD transmitter. There, security was proven under the assumption that this specific THA only affects the PM in the transmitter and leaves the other devices untouched. Therefore this result cannot be exported to decoy-state QKD and mdiQKD, where an additional method to modulate the intensity of the prepared signals is required. This is very often achieved via an intensity modulator (IM) inserted in series with the PM. Hence it can happen that partial information about the IM is leaked to Eve, similarly to what happens for the PM. This problem is common to any scheme using devices like PM and IM, such as the decoy-state BB84 protocol [43–51], bit commitment, oblivious transfer, secure identification [52], blind quantum computing [53] as well as device-independent QKD.

Here we introduce a general formalism to prove the security of most of the optical QKD systems using a PM and an IM in their transmitters that can leak the setting information in an arbitrary manner. As a specific example, we address the optical implementation of the standard decoy-state BB84 QKD protocol with three intensity settings [43–45] due to its extensive use of devices like PM and IM. However, our results can be straightforwardly adapted to any number of settings and to all the protocols mentioned above. Importantly, our approach is solely based on how the users' devices operate. For a given model of PM and IM, one could readily use our technique to calculate the resulting secret key rate of the system. This constitutes a fundamental step forward to guaranteeing the security of quantum cryptographic schemes using a PM, an IM or other analogous devices, in presence of information leakage.

To illustrate how our formalism applies to real QKD systems, we investigate a particular form of information leakage, i.e., a THA that is feasible with current technology. In particular, we consider that Eve injects a probe for each phase and intensity setting selected by the legitimate user and the back-reflected light is composed of coherent states of limited intensity.

The paper is organised as follows. In section 2 we review the main concepts of decoy-state QKD. In section 3 we present a general formalism to prove its security in the presence of any information leakage from both the PM and the IM. This formalism is then used in section 4 to study various THA that are feasible with current technology and to evaluate their effect on the system performance. Finally, section 5 includes a short discussion and section 6 concludes the paper with a summary. The paper also contains appendices with calculations that are needed to derive the results in the main text.

2. Decoy-state QKD

In decoy-state QKD, Alice prepares mixtures of Fock states with different photon number statistics, selected independently at random for every signal that is sent to Bob. These states can be prepared with practical light sources such as attenuated laser diodes, heralded spontaneous parametric downconversion sources and other practical single-photon sources. They can be formally described as:

$$\rho^{\gamma} = \sum_{n=0}^{\infty} p_n^{\gamma} \, |n\rangle\langle n|. \tag{1}$$

Here, p_n^{γ} is the photon number statistics, represented by the conditional probability that Alice emits a pulse with n photons when she chooses the intensity setting γ. The ket $|n\rangle$ denotes an n-photon Fock state. If Alice uses a source emitting phase-randomised weak coherent pulses (WCP), the photon number statistics is the Poisson distribution, $p_n^{\gamma} = e^{-\gamma}\gamma^n/n!$, with γ being the mean photon number.

For each intensity setting γ, there are two quantities which can be directly observed in the experiment: the gain $Q^{\gamma} = N_{\text{click}}^{\gamma}/N^{\gamma}$, where $N_{\text{click}}^{\gamma}$ represents the number of events where Bob observes a click in his measurement device given that Alice prepared the state ρ^{γ}, and N^{γ} is the number of signals sent by Alice in the

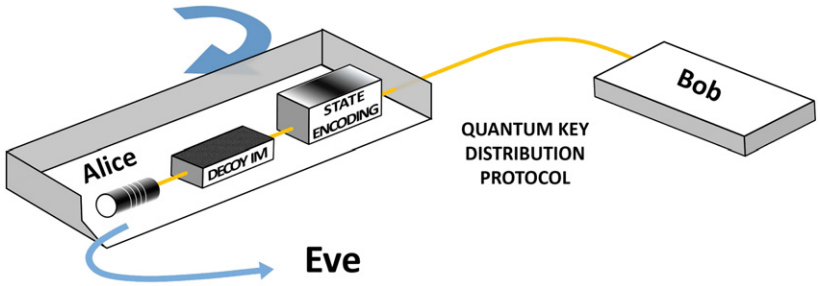

Figure 1. The users Alice and Bob run a QKD protocol with apparatuses that can have leakages (thin arrow in the figure). Any such leaked signal could be captured by Eve and used to steal private information. Eve can even actively shine high-power electromagnetic fields on the system (thick arrow in the figure) to trigger the emission of side-channel signals.

state ρ^{γ}, and the quantum bit error rate $E^{\gamma} = N^{\gamma}_{\text{error}}/N^{\gamma}_{\text{click}}$, where $N^{\gamma}_{\text{error}}$ denotes the number of errors observed by Bob given that Alice prepared the state ρ^{γ}. In the asymptotic limit of large N^{γ} both quantities can be written as a function of the yield Y_n and the error rate e_n of the n-photon signals as:

$$Q^{\gamma} = \sum_{n=0}^{\infty} p_n^{\gamma} Y_n,$$
$$E^{\gamma} = \frac{1}{Q^{\gamma}} \sum_{n=0}^{\infty} p_n^{\gamma} Y_n e_n, \tag{2}$$

for any value of γ. The unknown parameters in this set of linear equations are Y_n and e_n, and they can be estimated by solving equation (2).

Indeed, whenever Alice uses an infinite number of settings γ, any finite set of parameters Y_n and e_n can be estimated with arbitrary precision. If Alice and Bob are only interested in the value of Y_0, Y_1, and e_1, as is the case in QKD, it is possible to obtain a tight estimation of these three parameters with only a few different intensity settings [54]. A fundamental implicit requirement in the decoy-state analysis is that the variables Y_n and e_n are independent of the intensity setting γ. That is, the analysis assumes that Eve does not have any information about Alice's intensity setting choice at each given time. If Eve performs a THA against Alice's source, however, this necessary condition might not be longer satisfied and the security analysis of decoy-state QKD needs to be revised. This is done in the next section.

3. Trojan horse attacks against decoy-state QKD

In this section we present a general formalism to evaluate the security of decoy-state QKD against any information leakage from both the IM, which is used to generate decoy-states, and the PM employed to encode the bit and the basis information. Below we assume that such information leakage is due to an active Eve who launches a THA against the decoy-state transmitter. Note, however, that our analysis could be applied as well to any passive information leakage scenario.

In a THA Eve injects bright light pulses into Alice's device and measures the back-reflected light. This way she might obtain useful information about Alice's intensity and phase choices for each generated signal. This situation is illustrated in figure 1. As a first consequence, the yields Y_n and the error rates e_n might now become dependent on the intensity setting γ, and we will denote them as Y_n^{γ} and e_n^{γ}, respectively. The goal of this section is mainly to evaluate how much can these quantities differ from each other depending on the information leaked to Eve.

3.1. THA against the IM

Here we focus on the most widely used choice of intensity settings for the standard decoy-state BB84 protocol, where Alice randomly selects one of three possible intensities, denoted as γ_s, γ_v, and γ_w, with probability p_s, p_v, and p_w, respectively. However, our technique can be straightforwardly adapted to cover any number of decoy settings. We will denote as $\gamma^i \in \{\gamma_s, \gamma_v, \gamma_w\}$ the intensity setting selected by Alice in the ith instance of the protocol.

Eve's goal is to learn the value of γ^i for all instances i. For this, her most general THA can be described as follows. Eve first prepares a probe system $\mathrm{E_p}$, which might be entangled with an ancilla system E also in Eve's hands, and sends this system to Alice while she keeps E in a quantum memory. The system $\mathrm{E_p}$ may consist of many different pulses, each of them used to probe Alice's intensity setting each given time. Afterwards, Eve

performs a joint measurement on all the pulses emitted by Alice together with the systems E and the back-reflected light from E_p, which is denoted as E'_p.

Let us consider first the ith n-photon pulse emitted by Alice. Later on we will generalise this case to cover all her n-photon pulses. For this, let ρ_{n,γ^i} denote the joint state of Alice's ith n-photon pulse and the systems[6] E and E'_p. The state of E'_p may depend on all the intensity choices made by Alice, so does ρ_{n,γ^i}. Now, Eve's task for the ith pulse is to behave as different as possible according to Alice's intensity choice γ^i given the state ρ_{n,γ^i}. Therefore, we are interested in how well can Eve distinguish the intensity setting γ^i_j from γ^i_k and γ^i_l, with $j, k, l \in \{s, v, w\}$ and $j \neq k, l$ (note that here k might be equal to l). This can be solved using the trace distance argument [55], which says that the trace distance between probability distributions arising from any measurement on the states ρ_{n,γ^i_j} and $q_{nkl}\rho_{n,\gamma^i_k} + (1 - q_{nkl})\rho_{n,\gamma^i_l} := \sigma_{n,\gamma^i_{kl}}$ satisfies

$$\sum_{\omega\in\Omega} |\Pr(\omega|\rho_{n,\gamma^i_j}) - \Pr(\omega|\sigma_{n,\gamma^i_{kl}})| \leqslant 2d(\rho_{n,\gamma^i_j}, \sigma_{n,\gamma^i_{kl}}), \tag{3}$$

where Ω is a set of physical events that fulfills $\sum_{\omega\in\Omega}\Pr(\omega) = 1$, $d(\rho, \sigma) := \mathrm{Tr}\,|\rho - \sigma|/2$ denotes the trace distance between ρ and σ, $\Pr(\omega|\rho)$ is the conditional probability to obtain the event ω given the state ρ, and $q_{nkl} := p_k p_n^{\gamma_k}/(p_k p_n^{\gamma_k} + p_l p_n^{\gamma_l})$, with $k, l \in \{s, v, w\}$, is the conditional probability to have selected the intensity setting γ_k (among only γ_k and γ_l) given that the pulse contains n photons[7].

To prove the security of the decoy-state QKD system, we need to determine Bob's detection rates. This means that we are interested in the set $\Omega = \{\text{click}, \text{no click}\}$, where 'click' ('no click') represents a detection (no detection) outcome at Bob's side. That is, Eve must decide which of Alice's pulses will produce (or not produce) a 'click' at Bob's side before the quantum part of the protocol finishes. Here, $\Pr(\text{click}|\rho_{n,\gamma^i_j})$ is the conditional probability that Bob obtains a 'click' given ρ_{n,γ^i_j}. This probability may depend on the detection pattern observed by Bob in all the previous $i - 1$ pulses. By combining equation (3) with the fact that $\Pr(\text{click}) + \Pr(\text{no click}) = 1$ we find that

$$|\Pr(\text{click}|\rho_{n,\gamma^i_j}) - \Pr(\text{click}|\sigma_{n,\gamma^i_{kl}})| \leqslant d(\rho_{n,\gamma^i_j}, \sigma_{n,\gamma^i_{kl}}) := D^i_{n,j,k,l}. \tag{4}$$

Now, in order to relate the conditional probabilities that appear in equation (4) with the corresponding actual numbers, we first convert these probabilities into joint probabilities and then we take the sum over $i \in \{1, 2, \ldots, N\}$, being N the number of trials. In particular, let $\Pr(\text{click}, n, \gamma^i_j)$ denote the joint probability that Eve observes the state ρ_{n,γ^i_j} in the instance i and Bob obtains a 'click'. Then, from equation (4) we obtain that

$$\left| \sum_{i=1}^{N} \Pr(\text{click}, n, \gamma^i_j) - p_j p_n^{\gamma_j} \sum_{i=1}^{N} \left[q_{nkl} \frac{\Pr(\text{click}, n, \gamma^i_k)}{p_k p_n^{\gamma_k}} + (1 - q_{nkl}) \times \frac{\Pr(\text{click}, n, \gamma^i_l)}{p_l p_n^{\gamma_l}} \right] \right| \leqslant p_j p_n^{\gamma_j} N D_{n,j,k,l}, \tag{5}$$

where $D_{n,j,k,l} := 1/N\sum_{i=1}^{N} D^i_{n,j,k,l}$. Importantly, by using Azuma's inequality [56] (see appendix A), each term on the lhs of equation (5) approaches the actual numbers of the corresponding events except for a probability exponentially small in N. That is, we have that $\sum_{i=1}^{N}\Pr(\text{click}, n, \gamma^i_j)$ approaches the number of events, $N_{\text{click},n,\gamma_j}$, within N runs where Alice selects the intensity setting j, she emits an n-photon state, and Bob obtains a 'click' in his measurement device. This means that

$$|Y_n^{\gamma_j} - [q_{nkl}Y_n^{\gamma_k} + (1 - q_{nkl})Y_n^{\gamma_l}]| \leqslant D_{n,j,k,l}, \tag{6}$$

except for a probability exponentially small[8] in N, where the yields $Y_n^{\gamma_j}$ are defined as

$$Y_n^{\gamma_j} := \frac{N_{\text{click},n,\gamma_j}}{N p_j p_n^{\gamma_j}} \tag{7}$$

and similarly for $Y_n^{\gamma_k}$ and $Y_n^{\gamma_l}$. Note that in the special case where there is no information leakage about Alice's intensity choices, we have that $D_{n,j,k,l} = 0$ and, therefore, $Y_n^{\gamma_j} = Y_n^{\gamma_k} = Y_n^{\gamma_l} := Y_n$, which is the key assumption in the standard decoy-state method (see section 2).

The analysis for the error rates $e_n^{\gamma_j}$, with $j \in \{s, v, w\}$, is analogous. In particular, here we consider the set $\Omega = \{\text{click} \wedge \text{error}, \text{no click} \vee (\text{click} \wedge \text{no error})\}$, where 'click $\wedge$ error' represents a detection outcome at

[6] For example, if the emission of an n-photon pulse by Alice is independent of Eve's systems E and E'_p, then $\rho_{n,\gamma^i} = \hat{P}(|n\rangle) \otimes \rho_{\gamma^i}$, where the operator $\hat{P}(|\phi\rangle)$ is defined as $\hat{P}(|\phi\rangle) := |\phi\rangle\langle\phi|$ and ρ_{γ^i} represents the state of E and E'_p. This is the typical situation that one expects in practice.

[7] Note that when $k = l$ equation (3) implies that $\sum_{\omega\in\Omega}|\Pr(\omega|\rho_{n,\gamma^i_j}) - \Pr(\omega|\rho_{n,\gamma^i_k})| \leqslant 2d(\rho_{n,\gamma^i_j}, \rho_{n,\gamma^i_k})$ for all $j, k \in \{s, v, w\}$.

[8] Note that when $k = l$ equation (6) implies that $|Y_n^{\gamma_j} - Y_n^{\gamma_k}| \leqslant D_{n,j,k}$ with $D_{n,j,k} := 1/N\sum_{i=1}^{N} D^i_{n,j,k}$ and $D^i_{n,j,k} = d(\rho_{n,\gamma^i_j}, \rho_{n,\gamma^i_k})$.

Bob's side associated with an error, and 'no click $\vee$ (click $\wedge$ no error)' denotes a no detection outcome or a detection one associated with no error. Now, taking into account that $\Pr(\text{click} \wedge \text{error}) + \Pr[\text{no click} \vee (\text{click} \wedge \text{no error})] = 1$, and using a similar analysis as above, we find that

$$|Y_n^{\gamma_j} e_n^{\gamma_j} - [q_{nkl} Y_n^{\gamma_k} e_n^{\gamma_k} + (1 - q_{nkl}) Y_n^{\gamma_l} e_n^{\gamma_l}]| \leqslant D_{n,j,k,l}, \tag{8}$$

where the parameter $D_{n,j,k,l}$ is equal to that given in equation[9] (6), and $e_n^{\gamma_j}$ is defined as

$$e_n^{\gamma_j} := \frac{N_{\text{click}\wedge\text{error},n,\gamma_j}}{N_{\text{click},n,\gamma_j}} \tag{9}$$

and similarly for $e_n^{\gamma_k}$ and $e_n^{\gamma_l}$. Here, $N_{\text{click}\wedge\text{error},n,\gamma_j}$ represents the number of events, within N runs, where Alice selects the intensity setting j, she emits an n-photon state, and Bob obtains a 'click' associated to an error in his measurement device.

The formalism above is general in the sense that it can be applied to *any* THA against Alice's IM. However, to be able to evaluate equations (6)–(8) one needs to characterise the states ρ_{n,γ_j^i} that are accessible to Eve, and this might be difficult in general. These states are required to calculate the coefficients $D^i_{n,j,k,l}$ and, thus, the parameters $D_{n,j,k,l}$. In the next subsection we show that these parameters can in principle be estimated based solely on the behaviour of the IM.

3.1.1. Estimation of $D^i_{n,j,k,l}$

In order to upper bound the value of $D^i_{n,j,k,l}$ based only on how the IM operates, we consider the unitary operator that describes the action of Alice's IM when she selects a certain intensity setting γ_j^i for an instance i. Importantly, we assume that this operator characterises the behaviour of the IM on all the optical modes that it supports. That is, in general it acts on Alice's photonic system $\mathrm{A_p}$ (i.e., the signal states emitted by her laser), on some additional ancillary system $\mathrm{A_a}$ also in Alice's hands[10], and on Eve's probe system $\mathrm{E_p}$. Therefore, we will denote it as $\hat{U}^{\gamma_j^i}_{\mathrm{A_p},\mathrm{A_a},\mathrm{E_p}}$.

Let $|\Psi\rangle_{\mathrm{A_p},\mathrm{A_a},\mathrm{E},\mathrm{E_p}}$ be the joint state that describes Alice's and Eve's systems before the action of the IM. After applying the IM, the state $|\Psi\rangle_{\mathrm{A_p},\mathrm{A_a},\mathrm{E},\mathrm{E_p}}$ evolves according to the unitary transformation $\hat{\mathbb{1}}_{\mathrm{E}} \otimes \hat{U}^{\gamma_j^i}_{\mathrm{A_p},\mathrm{A_a},\mathrm{E_p}}$. Importantly, in order for the decoy-state method to work, this unitary transformation should produce an output signal with the system $\mathrm{A_p'}$ (which will be sent to Bob through the quantum channel once the bit and basis information are also encoded) prepared in a state that is diagonal in the Fock basis. Note here that the physical system corresponding to $\mathrm{A_p'}$ might not be the same as the one for the input system $\mathrm{A_p}$. This means, in particular, that

$$\hat{\mathbb{1}}_{\mathrm{E}} \otimes \hat{U}^{\gamma_j^i}_{\mathrm{A_p},\mathrm{A_a},\mathrm{E_p}} |\Psi\rangle_{\mathrm{A_p},\mathrm{A_a},\mathrm{E},\mathrm{E_p}} = \sum_n \sqrt{p_n^{\gamma_j^i}}\, |n^{\gamma_j^i}\rangle_{\mathrm{A_p'}} |\phi^{\gamma_j^i}_{n,\Psi}\rangle_{\mathrm{A_a'},\mathrm{E},\mathrm{E_p'}}. \tag{10}$$

Here, $p_n^{\gamma_j^i}$ denotes the probability of emitting an n-photon pulse in the ith instance of setting γ_j, and $\{|\phi^{\gamma_j^i}_{n,\Psi}\rangle_{\mathrm{A_a'},\mathrm{E},\mathrm{E_p'}}\}_n$ forms an orthonormal basis, i.e., we have that ${}_{\mathrm{A_a'},\mathrm{E},\mathrm{E_p'}}\langle\phi^{\gamma_j^i}_{n',\Psi}|\phi^{\gamma_j^i}_{n,\Psi}\rangle_{\mathrm{A_a'},\mathrm{E},\mathrm{E_p'}} = \delta_{n'n}$. Moreover, the physical systems for $\mathrm{A_a'}$ and $\mathrm{E_p'}$ might be different from those for $\mathrm{A_a}$ and $\mathrm{E_p}$, respectively. Also, note that in equation (10) we have made the general assumption that the photon mode of the n-photon state $|n^{\gamma_j}\rangle_{\mathrm{A_p'}}$ might be dependent on the setting γ_j^i.

Now, we focus on those joint states $|n^{\gamma_j^i}\rangle_{\mathrm{A_p}} |\phi^{\gamma_j^i}_{n,\Psi}\rangle_{\mathrm{A_a'},\mathrm{E},\mathrm{E_p'}}$ that contain n photons on Alice's photonic system $\mathrm{A_p'}$. Eve's task is to behave as differently as possible according to the intensity setting. We find, therefore, that $D^i_{n,j,k,l}$ can be upper bounded as

$$\begin{aligned} D^i_{n,j,k,l} \leqslant \mathrm{Sup}_{|\Psi\rangle_{\mathrm{A_p},\mathrm{A_a},\mathrm{E},\mathrm{E_p}}} & d(\mathrm{Tr}_{\mathrm{A_a'}}[\hat{P}(|n^{\gamma_j^i}\rangle_{\mathrm{A_p'}} |\phi^{\gamma_j^i}_{n,\Psi}\rangle_{\mathrm{A_a'},\mathrm{E},\mathrm{E_p'}})], \\ & \mathrm{Tr}_{\mathrm{A_a'}}[q_{nkl}\hat{P}(|n^{\gamma_k^i}\rangle_{\mathrm{A_p'}} |\phi^{\gamma_k^i}_{n,\Psi}\rangle_{\mathrm{A_a'},\mathrm{E},\mathrm{E_p'}}) \\ & + (1 - q_{nkl})\hat{P}(|n^{\gamma_l^i}\rangle_{\mathrm{A_p'}} |\phi^{\gamma_l^i}_{n,\Psi}\rangle_{\mathrm{A_a'},\mathrm{E},\mathrm{E_p'}})]), \end{aligned} \tag{11}$$

[9] If $k = l$ then equation (8) implies that $|Y_n^{\gamma_j} e_n^{\gamma_j} - Y_n^{\gamma_k} e_n^{\gamma_k}| \leqslant D_{n,j,k}$.

[10] The system $\mathrm{A_a}$ can account for the effect of the loss in Alice's transmitter. That is, we consider that the unitary operator describing her IM includes as well, together with its intrinsic loss, the effect of any optical attenuator, isolator and filter used by Alice to reduce the energy of the back-reflected light that goes to Eve.

where the operator $\hat{P}(|\phi\rangle) \coloneqq |\phi\rangle\langle\phi|$. This confirms that the description of Alice's IM is enough to guarantee security.

Of course, the formalism above can readily accept any particular assumption on the THA performed by Eve. For instance, in practical situations it may be over-pessimistic to take the supremum given in equation (11) over all possible states $|\Psi\rangle_{A_p,A_a,E,E_p}$. Instead, one might only consider signals of the form $|\Psi\rangle_{A_p,A_a,E,E_p} = |\phi\rangle_{A_p}\,|\varphi\rangle_{A_a}\,|\chi\rangle_{E,E_p}$, where $|\phi\rangle_{A_p}$, $|\varphi\rangle_{A_a}$ and $|\chi\rangle_{E,E_p}$ are pure states of the different systems. Indeed, this seems to be a natural assumption because Alice's systems A_p and A_a are typically independent from each other and also independent from those of Eve. In so doing, equation (11) might deliver tighter bounds for $D^i_{n,j,k,l}$.

In general, however, one cannot assume that Eve's state $|\chi\rangle_{E,E_p}$ is in a tensor product form. That is, it is not enough to just consider the system E_p that Eve sends to Alice (together with the back-reflected one) in order to guarantee security. This is so because when the supremum given in equation (11) is taken over all joint states $|\chi\rangle_{E,E_p}$ it usually results in a larger trace distance than that obtained when one considers product states. To improve the system performance, Alice might include additional optical elements to force $|\chi\rangle_{E,E_p}$ to be of product form. For example, she could perform a phase-randomisation on the system E_p (see, e.g., [58, 59]). This way all the off-diagonal elements of the state $|\chi\rangle_{E,E_p}$ in the Fock basis would vanish, and one could completely disregard system E. Moreover, mathematically, to remove all the off-diagonal elements leads to a significant decrease of the trace distance and, therefore, one expects a significant improvement of the secure key rate, as is confirmed in section 4.3.

3.2. THA against the PM

In this section, we review and extend the analysis of the THA against the PM carried out in [42]. The central observation is that the THA allows Eve to partially know Alice's choice of the basis. In other terms, the information leakage is in the form of basis information leaked out to the eavesdropper. This might cause the density matrices that describe Alice's output states to be *basis dependent*. Below, we provide a formalism to prove the security of the BB84 protocol in the presence of the most general THA against the PM.

We will assume that Alice's choice is random, independent of the IM and of the previous preparation instances. We define the Z basis by the orthogonal vectors $\{|0\rangle, |1\rangle\}$ and the X basis by $\{|+\rangle, |-\rangle\}$, where $|\pm\rangle \coloneqq (|0\rangle \pm |1\rangle)/\sqrt{2}$. We denote as $|\Psi^i_Z\rangle_{A_q,A_p,A_a,E,E'_p}$ ($|\Psi^i_X\rangle_{A_q,A_p,A_a,E,E'_p}$) the joint state that describes Alice's system and Eve's system for the THA given that Alice selected the Z (X) basis. Here, the superscript i refers to the ith signal generated by Alice, and the system A_q refers to a virtual qubit that is stored in Alice's lab. Examples of the states $|\Psi^i_Z\rangle_{A_q,A_p,A_a,E,E'_p}$ and $|\Psi^i_X\rangle_{A_q,A_p,A_a,E,E'_p}$ are the following

$$|\Psi^i_Z\rangle_{A_q,A_p,A_a,E,E'_p} = \frac{1}{\sqrt{2}}(|0\rangle_{A_q}\,|\Psi^i_{0_Z}\rangle_{A_p,A_a,E,E'_p} + |1\rangle_{A_q}\,|\Psi^i_{1_Z}\rangle_{A_p,A_a,E,E'_p}), \tag{12}$$

$$|\Psi^i_X\rangle_{A_q,A_p,A_a,E,E'_p} = \frac{1}{\sqrt{2}}(|+\rangle_{A_q}\,|\Psi^i_{0_X}\rangle_{A_p,A_a,E,E'_p} + |-\rangle_{A_q}\,|\Psi^i_{1_X}\rangle_{A_p,A_a,E,E'_p}). \tag{13}$$

Here, $|\Psi^i_{j_\alpha}\rangle_{A_p,A_a,E,E'_p}$ (with $j \in \{0, 1\}$ and $\alpha \in \{Z, X\}$) represents the state of systems A_p, A_a, E and E'_p for Alice's bit value j in her α basis. We have, therefore, that Alice's state preparation process can be equivalently described as follows. First, she decides which state ($|\Psi^i_Z\rangle_{A_q,A_p,A_a,E,E'_p}$ or $|\Psi^i_X\rangle_{A_q,A_p,A_a,E,E'_p}$) she prepares. Afterwards, she measures the virtual qubit A_q using the Z or the X basis, depending on the choice of the state. As long as the state preparation is expressed this way, one can consider any possible purification of the states $|\Psi^i_Z\rangle_{A_q,A_p,A_a,E,E'_p}$ or $|\Psi^i_X\rangle_{A_q,A_p,A_a,E,E'_p}$. For instance, one may consider $|\Psi^i_X\rangle_{A_q,A_p,A_a,E,E'_p} = \frac{e^{i\nu}}{\sqrt{2}}(|-\rangle_{A_q}\,|\Psi^i_{0_X}\rangle_{A_p,A_a,E,E'_p} + |+\rangle_{A_q}\,|\Psi^i_{1_X}\rangle_{A_p,A_a,E,E'_p})$ with $\nu \in [0, 2\pi)$ being a global phase. Note that we can consider this state because the reduced density operator for systems A_p, A_a, E and E'_p is the same as that of equation (13). The optimal solution is the purification that maximises the key generation rate.

In a security proof, it is essential to determine the phase error rate, which is the parameter needed in the privacy amplification step of the protocol. The phase error rate is the fictitious bit error rate that Alice and Bob would have obtained if Alice had measured the system A_q with the X basis and Bob had used the X basis given the preparation of $|\Psi^i_Z\rangle_{A_q,A_p,A_a,E,E'_p}$. Intuitively, if the states $|\Psi^i_Z\rangle_{A_q,A_p,A_a,E,E'_p}$ and $|\Psi^i_X\rangle_{A_q,A_p,A_a,E,E'_p}$ are close enough to each other, then the phase error rate should be close to the X basis error rate which is obtained in the actual experiment. Below, we make this argument more rigorous by using the analysis presented in [61]. For this, we will assume that the basis choice is done in a coherent manner, i.e., Alice first prepares the joint system

$$|\Psi^i\rangle_{A_c,\,A_q,A_p,A_a,E,E'_p} = \frac{1}{\sqrt{2}}(|0\rangle_{A_c}\,|\Psi^i_Z\rangle_{A_q,A_p,A_a,E,E'_p} + |1\rangle_{A_c}\,|\Psi^i_X\rangle_{A_q,A_p,A_a,E,E'_p}), \tag{14}$$

where the system A_c is the so-called 'quantum coin' [60]. Importantly, the phase error rate is related to the X basis measurement on the quantum coin. To derive the formula for the estimation of the phase error rate, we

consider the following fictitious protocol. In particular, for the ith trial of the protocol, Alice and Eve prepare their systems in the state $|\Psi^i\rangle_{A_c,A_q,A_p,A_a,E,E'_p}$, Alice keeps systems A_a, A_q and A_c in her hands, and sends system A_p to Bob. At the reception side, Bob receives some optical systems after Eve's intervention, and he performs the X basis measurement. In addition, Alice performs the X basis measurement on the system A_q. Then, Alice randomly chooses between the Z or the X basis with equal probability to measure her quantum coin A_c. Here, note that, from equation (14), when Alice chooses the Z basis to measure the coin and the result is '0' ('1'), this is equivalent to Alice and Eve directly preparing the state $|\Psi^i_Z\rangle_{A_q,A_p,A_a,E,E'_p}$ ($|\Psi^i_X\rangle_{A_q,A_p,A_a,E,E'_p}$). Next, we apply the Bloch sphere bound [62] for probability distributions to those instances where Bob obtained a click event. In particular, we first apply this bound separately to the events with the X basis error and to those with no X basis error. We obtain the following two inequalities

$$1 - 2\Pr^i(X_{Ac} = -|X - \text{Error}) \leqslant 2\sqrt{\Pr^i(Z_{Ac} = 1|X - \text{Error})(1 - \Pr^i(Z_{Ac} = 1|X - \text{Error}))}, \tag{15}$$

$$1 - 2\Pr^i(X_{Ac} = -|\text{No X} - \text{Error}) \leqslant 2\sqrt{\Pr^i(Z_{Ac} = 1|\text{No X} - \text{Error})(1 - \Pr^i(Z_{Ac} = 1|\text{No X} - \text{Error}))}. \tag{16}$$

Here, $\Pr^i(X_{Ac} = -|X - \text{Error})$ is the conditional probability of observing the outcome '−' when performing the X basis measurement on the quantum coin given that there is a X basis error; $\Pr^i(Z_{Ac} = 1|X - \text{Error})$ is the conditional probability of observing the outcome '1' when performing the Z basis measurement on the quantum coin given that there is a X basis error; and the other probabilities are defined similarly. Next, we multiply both inequalities by the term $\Pr^i(\text{click})$, which is the probability that Bob obtains a 'click' in his measurement apparatus, and after combining equations (15) and (16) we obtain [61]

$$\Pr^i(\text{click}) - 2\Pr^i(X_{A_c} = -) \leqslant 2\sqrt{\Pr^i(X, X - \text{Error})\Pr^i(Z, X - \text{Error})} + 2\sqrt{\Pr^i(X, \text{No X} - \text{Error})\Pr^i(Z, \text{No X} - \text{Error})}, \tag{17}$$

where $\Pr^i(X_{A_c} = -)$ is the probability that the measurement result on the quantum coin is '−', $\Pr^i(X, X - \text{Error})$ is the joint probability of selecting the Z basis to measure the quantum coin and obtaining the result '1' (which implies the preparation of the state $|\Psi^i_X\rangle_{A_q,A_p,A_a,E,E'_p}$), and observing a bit error in Alice's and Bob's X basis measurement. The probability $\Pr^i(Z, X - \text{Error})$ is the fictitious joint probability of selecting the Z basis to measure the quantum coin, and obtaining the result '0' (which implies the preparation of the state $|\Psi^i_Z\rangle_{A_q,A_p,A_a,E,E'_p}$), and observing a bit error in Alice's and Bob's X basis measurement. Actually, this last probability is the phase error rate. The probabilities $\Pr^i(X, \text{No X} - \text{Error})$ and $\Pr^i(Z, \text{No X} - \text{Error})$ are defined in a similar way (see [61] for further details). Note that in order to obtain equation (17) from equations (15) and (16) we have used the fact that $\Pr^i(X_{Ac} = -,\text{click}) \leqslant \Pr^i(X_{Ac} = -)$, where $\Pr^i(X_{Ac} = -, \text{click})$ represents the joint probability that the measurement result on the quantum coin is '−' and Bob obtains a 'click' event with his measurement. Importantly, the probability $\Pr^i(X_{A_c} = -)$ characterises how close are the states $|\Psi^i_Z\rangle_{A_q,A_p,A_a,E,E'_p}$ and $|\Psi^i_X\rangle_{A_q,A_p,A_a,E,E'_p}$. Specifically, by choosing an appropriate global phase for $|\Psi^i_X\rangle_{A_q,A_p,A_a,E,E'_p}$, from equation (14) we have that

$$\Pr^i(X_{A_c} = -) = \frac{1}{2}(1 - |_{A_q,A_p,A_a,E,E'_p}\langle\Psi^i_Z|\ \Psi^i_X\rangle_{A_q,A_p,A_a,E,E'_p}|). \tag{18}$$

The term $|_{A_q,A_p,A_a,E,E'_p}\langle\Psi^i_Z|\ \Psi^i_X\rangle_{A_q,A_p,A_a,E,E'_p}|$ can be upper-bounded by the fidelity between the Z basis state and the X basis state. This means that equation (17) gives us the phase error probability taking into account the 'closeness' between the two basis states. To relate the probabilities with the actual number of the corresponding events, we first use the concavity of the square root function and we take the sum over $i \in \{1, 2, \ldots, N\}$, with N being the number of pulses sent in the fictitious protocol. In so doing, we find that

$$\sum_{i=1}^{N}\Pr^i(\text{click}) - 2\sum_{i=1}^{N}\Pr^i(X_{A_c} = -) \leqslant 2\sqrt{\left[\sum_{i=1}^{N}\Pr^i(X, X - \text{Error})\right]\left[\sum_{i=1}^{N}\Pr^i(Z, X - \text{Error})\right]} + 2\sqrt{\left[\sum_{i=1}^{N}\Pr^i(X, \text{No X} - \text{Error})\right]\left[\sum_{i=1}^{N}\Pr^i(Z, \text{No X} - \text{Error})\right]}. \tag{19}$$

Next, we apply Azuma's inequality [56] (see appendix A). We obtain, therefore, that except for a probability exponentially small in N each sum of the probability distributions approaches the actual number of the corresponding events in N trials. That is

$$1 - 2\frac{N_{\mathrm{X}_{\mathrm{A_c}}=-}}{N_{\mathrm{click}}} \leqslant 2\sqrt{\frac{N_{\mathrm{X,X-Error}}}{N_{\mathrm{click}}}\frac{N_{\mathrm{Z,X-Error}}}{N_{\mathrm{click}}}} + 2\sqrt{\frac{N_{\mathrm{X,No\ X-Error}}}{N_{\mathrm{click}}}\frac{N_{\mathrm{Z,No\ X-Error}}}{N_{\mathrm{click}}}}, \tag{20}$$

where N_g denotes the number of instances associated to the event g. Importantly, here $N_{\mathrm{Z,X-Error}}/N_{\mathrm{click}}$ is related to the phase error rate, that is, the rate of choosing the Z basis and having the phase error, and $N_{\mathrm{X,X-Error}}/N_{\mathrm{click}}$ is the observed ratio of choosing the X basis and having a bit error. As for $N_{\mathrm{X}_{\mathrm{A_c}}=-}$, we have that except for a probability exponentially small in N the following inequality is satisfied

$$N_{\mathrm{X}_{\mathrm{A_c}}=-} \leqslant \sum_{i=1}^{N}\frac{1 - |_{\mathrm{A_q,A_p,A_a,E,E_p'}}\langle\Psi_{\mathrm{Z}}^i|\ \Psi_{\mathrm{X}}^i\rangle_{\mathrm{A_q,A_p,A_a,E,E_p'}}|}{2} \leqslant \frac{N}{2}[1 - \min_i |_{\mathrm{A_q,A_p,A_a,E,E_p'}}\langle\Psi_{\mathrm{Z}}^i|\ \Psi_{\mathrm{X}}^i\rangle_{\mathrm{A_q,A_p,A_a,E,E_p'}}|]. \tag{21}$$

This is so because we can directly calculate the probability $\Pr^i(\mathrm{X}_{\mathrm{A_c}} = -)$ from equation (14). Therefore, if Alice and Bob know the minimum overlap between the states $|\Psi_{\mathrm{X}}^i\rangle_{\mathrm{A_q,A_p,A_a,E,E_p'}}$ and $|\Psi_{\mathrm{Z}}^i\rangle_{\mathrm{A_q,A_p,A_a,E,E_p'}}$ they can estimate the value of the phase error rate even if Eve performs the most general THA against the PM. The estimation of such overlap, however, might be difficult in general as one would need to know Eve's ancilla state. To overcome this problem, we proceed like in the previous section and we reformulate the formalism above based only on how the PM operates.

For this, note that $|\Psi_{\mathrm{Z}}^i\rangle_{\mathrm{A_q,A_p,A_a,E,E_p'}}$ and $|\Psi_{\mathrm{X}}^i\rangle_{\mathrm{A_q,A_p,A_a,E,E_p'}}$ can be expressed as

$$|\Psi_{\zeta}^i\rangle_{\mathrm{A_q,A_p,A_a,E,E_p'}} := \hat{\mathbb{1}}_{\mathrm{A_q,E}} \otimes \hat{U}^{\zeta,i}_{\mathrm{A_p,A_a,E_p}}\ |\Psi\rangle_{\mathrm{A_q,A_p,A_a,E,E_p}}, \tag{22}$$

where $\zeta \in \{\mathrm{X}, \mathrm{Z}\}$, and $\hat{U}^{\zeta,i}_{\mathrm{A_p,A_a,E_p}}$ is the ith unitary[11] transformation associated to the PM. It supports Alice's photonic system $\mathrm{A_p}$ and her ancilla $\mathrm{A_a}$, and Eve's ancilla E together with her probe system $\mathrm{E_p}$. With this unitary transformation, the overlap between $|\Psi_{\mathrm{Z}}^i\rangle_{\mathrm{A_q,A_p,A_a,E,E_p'}}$ and $|\Psi_{\mathrm{X}}^i\rangle_{\mathrm{A_q,A_p,A_a,E,E_p'}}$ for the ith instance can be lower-bounded as

$$\mathrm{Inf}_{|\Psi\rangle_{\mathrm{A_q,A_p,A_aE,E_p}}}\ |_{\mathrm{A_q,A_p,A_a,E,E_p}}\langle\Psi|\ \hat{U}^{\mathrm{Z},i\dagger}_{\mathrm{A_p,A_a,E_p}}\hat{U}^{\mathrm{X},i}_{\mathrm{A_p,A_a,E_p}}\ |\Psi\rangle_{\mathrm{A_q,A_p,A_a,E,E_p}}|, \tag{23}$$

which is independent of the state. Note that here we have used the infimum because the unitary operator could support a mode in a Hilbert space containing an arbitrary number of photons. Therefore, equation (20) can be written as

$$1 - \frac{N}{N_{\mathrm{click}}}(1 - \min_i \mathrm{Inf}_{|\Psi\rangle_{\mathrm{A_q,A_p,A_aE,E_p}}}\ |_{\mathrm{A_q,A_p,A_a,E,E_p}}\langle\Psi|\ \hat{U}^{\mathrm{Z},i\dagger}_{\mathrm{A_p,A_a,E_p}}\hat{U}^{\mathrm{X},i}_{\mathrm{A_p,A_a,E_p}}\ |\Psi\rangle_{\mathrm{A_q,A_p,A_a,E,E_p}}|) \leqslant 2\sqrt{\frac{N_{\mathrm{X,X-Error}}}{N_{\mathrm{click}}}\frac{N_{\mathrm{Z,X-Error}}}{N_{\mathrm{click}}}} + 2\sqrt{\frac{N_{\mathrm{X,No\ X-Error}}}{N_{\mathrm{click}}}\frac{N_{\mathrm{Z,No\ X-Error}}}{N_{\mathrm{click}}}}. \tag{24}$$

Finally, we use

$$\delta_{\mathrm{X-Error|X}} := \frac{N_{\mathrm{X,X-Error}}}{N_{\mathrm{X}}}, \qquad \delta_{\mathrm{No\ X-Error|X}} := \frac{N_{\mathrm{X,No\ X-Error}}}{N_{\mathrm{X}}}, \qquad \delta_{\mathrm{X-Error|Z}} := \frac{N_{\mathrm{Z,X-Error}}}{N_{\mathrm{Z}}}, \qquad \delta_{\mathrm{No\ X-Error|Z}} := \frac{N_{\mathrm{Z,No\ X-Error}}}{N_{\mathrm{Z}}}, \tag{25}$$

where N_{Z} (N_{X}) is the number of events where Alice's Z-basis measurement outcome on the quantum coin is '0' ('1'). That is, Alice prepares the Z-basis (X-basis) state and Bob detects signals in the Z-basis (X-basis) in the actual protocol (recall that the virtual protocol concentrates only on the basis matched events). Then, by taking into account that $\sqrt{x(1-x)} \leqslant 1/2$ for $0 \leqslant x \leqslant 1$, we obtain the following modified inequality

$$1 - \frac{N}{N_{\mathrm{click}}}(1 - \min_i \mathrm{Inf}_{|\Psi\rangle_{\mathrm{A_q,A_p,A_aE,E_p}}}\ |_{\mathrm{A_q,A_p,A_a,E,E_p}}\langle\Psi|\ \hat{U}^{\mathrm{Z},i\dagger}_{\mathrm{A_p,A_a,E_p}}\hat{U}^{\mathrm{X},i}_{\mathrm{A_p,A_a,E_p}}\ |\Psi\rangle_{\mathrm{A_q,A_p,A_a,E,E_p}}|) \leqslant \sqrt{\frac{N_{\mathrm{X}}\delta_{\mathrm{X-Error|X}}}{N_{\mathrm{click}}}\frac{N_{\mathrm{Z}}\delta_{\mathrm{X-Error|Z}}}{N_{\mathrm{click}}}} + \sqrt{\frac{N_{\mathrm{X}}(1-\delta_{\mathrm{X-Error|X}})}{N_{\mathrm{click}}}\frac{N_{\mathrm{Z}}(1-\delta_{\mathrm{X-Error|Z}})}{N_{\mathrm{click}}}}. \tag{26}$$

Remember that N_{click} represents the number of detected events by Bob in the *actual* protocol since the quantum coins have been measured along the Z basis, which corresponds to the case in the actual protocol. Therefore, we have that the rhs of this equation is consistent with the results presented in [61].

[11] Similar to the IM, in general, the PM and other devices, may be correlated in their operations. In this case, this unitary transformation could depend on all the previous intensity choices that Alice has already made.

Like in the previous section, note that the formalism above can readily accept any assumption on the THA. For example, if one considers a specific THA against the PM where Alice and Bob know the fidelity $F_{X,Z}$ between the two density matrices describing the output states for the X and Z bases, we have that

$$1-\frac{N}{N_{\text{click}}}(1-F_{X,Z})\leqslant\sqrt{\frac{N_X\delta_{X-\text{Error}|X}}{N_{\text{click}}}\frac{N_Z\delta_{X-\text{Error}|Z}}{N_{\text{click}}}}+\sqrt{\frac{N_X(1-\delta_{X-\text{Error}|X})}{N_{\text{click}}}\frac{N_Z(1-\delta_{X-\text{Error}|Z})}{N_{\text{click}}}}, \tag{27}$$

which is essentially the result obtained in [42]. This means in particular that with the estimation of the fidelity given for an explicit THA, as the one considered in the next section, one can readily obtain the phase error rate and therefore the secure key rate of a QKD system endowed with a leaky PM.

Until now we have discussed the scenario where the THA against the IM and the PM acts independently on these two devices. However, in general, the IM and the PM might present correlations which could be exploited by Eve in a joint THA. More specifically, the leaked information might be dependent on both the intensity setting and the bit and basis choices. This situation is addressed in appendix B, where we discuss how to adapt the formalism above to also cover this case.

4. Simulation of the key generation rate

In order to apply the theoretical description to a practical case, we treat the THA as a particular form of information leakage, actively caused by the eavesdropper. We draw a realistic worst-case scenario following the line of [42], where a THA targeting the PM placed in Alice's box was studied. Here, we review this argument and employ it to any other device that is actively modulated in the transmitting unit, in particular to the IM that is commonly employed to run a decoy-state protocol. We assume that Eve uses a continuous-wave (CW) high-power laser to probe a QKD transmitter. The suitability of a CW laser for the THA is due to a twofold reason. Firstly, it is less destructive than a pulsed laser [63], so it is less easily detectable by Alice and Bob. Secondly, a CW laser is not less efficient than a pulsed laser in probing devices that are modulated according to a non-return-to-zero (NRZ) logic, and assuming NRZ modulation for the transmitter's devices is a conservative choice [42]. Also, it is apparent that the THA is enhanced if the power of Eve's laser is as large as possible, because this maximises the amount of back-reflected light for any fixed reflectivity of the transmitting unit. Therefore we can think that Eve's laser is operated well above threshold.

A consequence of these preliminary considerations is that it is not too restrictive in practice to consider a THA performed with a CW laser operated well above threshold. In turn, such a laser emits light in a state that is closely approximated by a single-mode coherent state [64]. We will therefore assume in this section that Eve uses high-intensity single-mode coherent states to perform the THA. Formally, we write the input coherent state as $|\beta' e^{i\theta'}\rangle$, where β' is a real number representing the amplitude of the input light and θ' is an arbitrary phase that can be set equal to zero without loss of generality. Notice that even if Eve's laser is CW, it still makes sense to use the expression 'light pulse' for Eve's light, as a light pulse is temporally defined by Eve to match the modulation period of the transmitter's devices. When a coherent state of light enters the QKD transmitter, it undergoes transformations that are linear and cannot change its photon statistics. So the light back-reflected to Eve will still be in a coherent state, which we indicate as:

$$|\beta_{\gamma_j} e^{i\theta_{\gamma_j}}\rangle. \tag{28}$$

In this case, the real numbers β_{γ_j} and θ_{γ_j} are amplitude and phase, respectively, of the light back-reflected to Eve, which can depend on the intensity setting of the transmitter, γ_j. Notice though that they are assumed not to depend on the particular instance i of the preparation. Moreover, in writing equation (28), we assume that there is no entanglement between Alice's system A_p and Eve's probe system E'_p. Therefore we term 'individual' this particular class of THA.

In the next sections, we will simulate the secure key rate of a typical decoy-state QKD system against the individual THA, in three different cases of practical interest, with the aim to provide security guidelines of immediate use in QKD experiments. The three cases correspond to different assumptions about the state in equation (28), which will be described in detail in the next sections 4.1–4.3. These cases will be also schematically summarised in figure 5, at the end of this section. However, figure 5 could even be used as an introductory scheme to our models instead, as it conveniently displays the assumptions underlying the simulations.

To draw the simulations, the main ingredient is the characterisation of the transmitters' modulators, which, as discussed in the previous section, leads to upper bound the trace distance between the different settings of the modulators in the presence of leaked information, as described by equation (11) (see also appendices C and D). In practice, this often translates into defining the modes transmitted by the modulators and their attenuation

Table 1. Experimental parameters used in the simulation of the secure key rate. The associated physical model is explained in appendix E. The values reported in the table are commonly met in a fibre-based QKD setup, see e.g. [65]. The intensity parameters γ_s and γ_v are not displayed in the table as they are optimised numerically at every distance. The parameter γ_w is set equal to a constant value to reduce the parameter space of the simulation. Its effect on the key rate is marginal.

q	e_d	p_d	η_B	η_{det}	α	γ_w	$f(E^{\gamma_s})$
1	0.01	5×10^{-6}	0.5	0.25	0.2	5×10^{-4}	1.2

coefficients. Then, a specific protocol can be considered and its secure key rate estimated. In the simulations, we will consider the following lower bound to the asymptotic secure key rate of the decoy-state BB84 protocol [3]:

$$K \geqslant \max_{\Gamma_A} \min_{\Gamma_E} q\{p_0^{\gamma_s} Y_{0L}^{\gamma_s} + p_1^{\gamma_s} Y_{1L}^{\gamma_s}[1 - h(e_{1U}^{\gamma_s})] - f(E^{\gamma_s}) Q^{\gamma_s} h(E^{\gamma_s})\}, \tag{29}$$

where Γ_A and Γ_E are the spaces of the parameters controlled by Alice and by Eve, respectively. In the simulation, we will use $\Gamma_A = \{\gamma_s, \gamma_v\}$ and $\Gamma_E = \{\theta_{\gamma_j}\}$, and assume without loss of generality that $\gamma_s \geqslant \gamma_v \geqslant \gamma_w$ and $\theta_{\gamma_s} = 0$, $\theta_{\gamma_v} \in [0, 2\pi]$, $\theta_{\gamma_w} \in [\theta_{\gamma_v}, 2\pi]$. Here, as for γ_w and β_{γ_j}, we will fix them to particular constant values in the simulation. In equation (29), the key is distilled only from the signal states; q is the efficiency of the protocol; $p_0^{\gamma_s} = e^{-\gamma_s}$ and $p_1^{\gamma_s} = \gamma_s e^{-\gamma_s}$; $Y_{0L}^{\gamma_s}$ and $Y_{1L}^{\gamma_s}$ ($e_{1U}^{\gamma_s}$) are lower (upper) bounds for $Y_0^{\gamma_s}$ and $Y_1^{\gamma_s}$, respectively, ($e_1^{\gamma_s}$) is defined in section 3; $f(E^{\gamma_s})$ is the efficiency of the error correction protocol; $h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary Shannon entropy function. All the parameters used in the simulation are listed in table 1 and the associated physical model for the quantum transmission is described in appendix E. The calculation of K passes through the estimation of $Y_{0L}^{\gamma_s}$, $Y_{1L}^{\gamma_s}$ and $e_{1U}^{\gamma_s}$, which is performed by numerical constrained optimisation as explained in appendix C.

4.1. Individual THA—Case 1

As mentioned in section 3, Eve's goal in a THA is to maximise the difference between the states leaked out of the transmitter. Because these are represented by the coherent state in equation (28), Eve's task is simpler when the intensity of the relevant states is larger, as this makes the states more orthogonal. Therefore, the first scenario we consider is one in which we over-estimate the intensity of the leaked states so to draw a consistent worst-case scenario for the individual THA. Suppose that the users characterise their apparatus and find that the intensity of the leaked signals is always upper bounded by a certain value I_{max}. This could be the result of an experiment aimed at characterising the worst-case reflectivity of the transmitter as a whole, without specifically addressing the individual devices inside the transmitting unit. Because in the estimation of the secure key rate, equation (29), we assume that the parameters θ_{γ_j} are entirely controlled by Eve, it is conservative to set the intensities of the states leaked out from the transmitter as follows:

$$\beta_{\gamma_s}^2 = \beta_{\gamma_v}^2 = \beta_{\gamma_w}^2 = \beta^2 = I_{max}. \tag{30}$$

The detailed calculation of the trace distance terms $D_{n,j,k,l}$ for the leaked states under the settings of equation (30) is given in appendix D.1. Then, the key rate in equation (29) is numerically simulated and the result is plotted in figure 2 as a function of the distance between the users. The colours correspond to different values of the parameter I_{max}. The black solid line represents the ideal case of no information leakage. When the information leakage intensity is lower than 10^{-6} photons/pulse, it is always possible to distill a secure quantum key, even in presence of the THA. When $I_{max} = 10^{-6}$, the key rate distilled from our security proof remains positive up to distances of about 30 km. This can be compared with implementation without decoy states, where a single unmodulated intensity is used. In this case, the so-called GLLP security proof [60] applies, and the corresponding key rate is depicted in figure 2 as a dashed black line. When I_{max} is smaller than 10^{-12}, the key rate in presence of a THA approaches closely that of a perfectly shielded system over short and medium-range distances, whereas it deviates from ideal over longer distances. In this latter case, a non-negligible amount of additional privacy amplification is required to protect the system against the THA. In the same figure, we also include dashed coloured lines to represent the secure key rate in presence of a THA that targets simultaneously the IM and the PM enclosed in a QKD transmitter. For that, we conservatively assumed that Eve gets the same amount of back-reflected light, I_{max}, from the IM and the PM separately, so to maximise her information gain about each modulator. As it is apparent from figure 2, the lines corresponding to this case are almost perfectly overlapping with the lines corresponding to having only the IM attacked by the THA. This suggests that protecting the IM of a decoy-state QKD transmitter against the THA is more challenging than protecting the PM alone. In fact, an optical isolation is required for the IM that is orders of magnitudes larger than the one for the PM. Even so, this difference is not larger than about 60 dB [42]. This roughly corresponds to the optical isolation displayed by an inexpensive commercially available component like a dual-stage optical isolator. Hence this solution is well within the feasibility range of current technology.

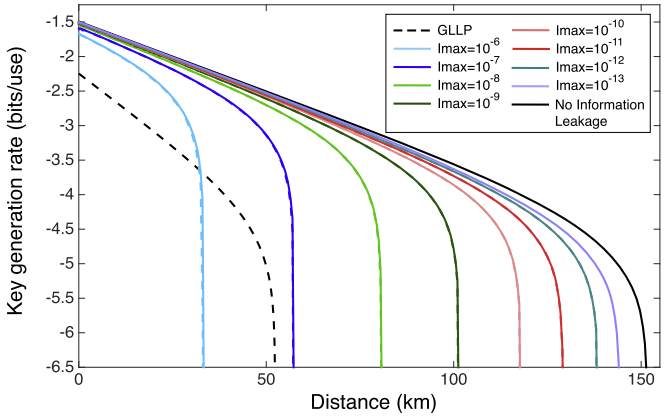

Figure 2. Secure key rate versus distance in presence of a THA targeting the modulating devices of a QKD transmitter. Each colour corresponds to a different value of the intensity of the leaked light, $I_{\max}$. The depicted key rate is for the worst-case of a single value of $I_{\max}$ bounding all the intensity settings in the transmitter, see equation (30) in the main text. The solid lines are for a leakage due only to the IM, while the dashed lines, visible for $I_{\max}$ equal to 10^{-6}, 10^{-7} and 10^{-8}, are for the total leakage coming from IM and PM simultaneously. For every distance, the key rate is minimised over the angles θ_{γ_j}, controlled by Eve, and maximised over the amplitudes γ_s and γ_v, controlled by Alice. All the parameters used in the simulation are listed in table 1.

4.2. Individual THA—Case 2

In the previous section, we considered a worst-case assumption for the amount of light leaked out of the QKD transmitter, equation (30). In that model, the leaked intensity was independent of the inner setting of the transmitter. On the one hand, this permits to bypass the precise characterisation of the QKD setup. On the other hand, it neglects a few physical considerations that can considerably improve the key rate. For example, the fraction of Eve's light that is back-reflected by a component that precedes the modulators in the transmitter's architecture does not contribute to the THA. A second important consideration is that, according to the initial worst-case scenario drawn for the individual THA, the modulators are driven with a NRZ logic. This entails that most of the time during the encoding process the modulators' medium is non-reflective, as its refractive index is homogeneous and constant between two consecutive NRZ modulation values. Hence, the THA has to be executed exploiting not the reflectivity of the IM (or PM), but that of the interfaces coming after it in the transmitter's architecture instead. Specifically, the THA would run as follows[12]: Eve's light passes through the IM a first time; it hits an interface placed after the IM and is reflected back from it towards the IM; it passes through the IM a second time and is finally leaked out of the QKD system into Eve's hands. During this two-way trip through the IM, Eve's light undergoes the same changes as the signals prepared by the transmitter for a normal QKD session. Therefore the leaked light is now highly informative of the inner settings of the transmitter.

In principle, a two-way round trip through a NRZ-modulated IM entails a double attenuation of Eve's light. However, because attenuation plays against Eve in a THA, it is conservative to assume that Eve's light is attenuated only once by the IM. To fix the ideas we can think that it passes unattenuated through the IM on the forward path and then is attenuated on the backward path in exactly the same way as the legitimate signals are. In this new scenario, the settings for the amplitudes of the leaked light are:

$$\beta^2_{\gamma_s} = I_{\max}, \qquad \beta^2_{\gamma_v} = \frac{\gamma_v}{\gamma_s} I_{\max}, \qquad \beta^2_{\gamma_w} = \frac{\gamma_w}{\gamma_s} I_{\max}. \tag{31}$$

Hence, differently from the previous case, Alice's modulation of the intensity directly affects now the information leaked to the eavesdropper for any fixed value of $I_{\max}$. The detailed calculation of the trace distance terms $D_{n,j,k,l}$ for the leaked states under equation (31) is given in appendix D.2.

In figure 3, we plot the secure key rate as a function of the distance between the users, varying the parameter $I_{\max}$. The key rate has improved with respect to that in figure 2. For the largest intensity of the leakage in the figure, $I_{\max} = 10^{-6}$, the key rate derived from our security proof reaches about 60 km distance and is always better than the one attained with the GLLP approach. Moreover, for a leakage intensity $I_{\max} = 10^{-12}$, the key rate is nearly indistinguishable from the rate of an ideally shielded system (black solid line in figure 3) up to about 100 km, that is 70% of the maximum transmission distance.

As in the previous case, we include in the figure the simulation of the key rate under a THA simultaneously run against the IM and the PM (dashed coloured lines in figure 3). Again, the THA against the PM only marginally affects the overall key rate. Therefore the countermeasure to information leakage based on readily

[12] We explicitly consider the IM in this description but the argument also applies to the PM.

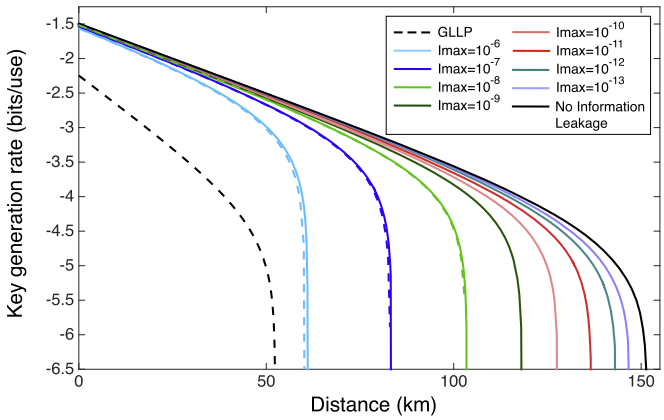

Figure 3. Secure key rate versus distance in presence of a THA targeting the modulating devices of a QKD transmitter. Each colour corresponds to a different value of $I_{\max}$. The depicted key rate is obtained when the intensity of the leaked light is modulated in the same way as for the standard light pulses in decoy-state QKD, see equation (31) in the main text. The solid lines are for a leakage due only to the IM, while the dashed lines, visible for $I_{\max}$ equal to 10^{-6}, 10^{-7} and 10^{-8}, correspond to the total leakage coming from the IM and the PM of the transmitter simultaneously. For every distance, the key rate is minimised over the angles θ_{γ_j}, controlled by Eve, and maximised over the amplitudes γ_s and γ_v, controlled by Alice. All the parameters used in the simulation are listed in table 1.

available optical isolators, discussed in the previous section 4.1, still applies here. Indeed, this solution becomes even more effective in the realistic scenario described in the present section, due to the better secure key rate shown in figure 3 in comparison with the worst-case key rate presented in figure 2.

4.3. Individual THA—Case 3

In this section, we further improve the key rate under a THA by considering the phase randomisation of Eve's signal, as discussed in section 3.1.1. Phase randomisation can drastically reduce the dangerousness of the THA as it removes any residual entanglement with the eavesdropper's probes, and we can expect higher key with the phase randomisation due to the non-existence of the off-diagonal elements. However, on the other hand, one has to be very careful about how phase randomisation is implemented, as this could open new loopholes. For example, if it is realised by adding a supplementary modulator to the system, Eve could first direct the THA against this new device to learn the phase information, and then address the PM and the IM as in the non-phase-randomised case, thus suppressing all the benefits due to the randomisation of the phase.

However, we showed in the previous sections that the THA against the PM is less effective than the one against the IM. Therefore, in order to improve the performance of the system against the THA, it is more important to randomise the phase of Eve's light directed against the IM than the one against the PM. This offers an alternative, possibly more robust, way to implement phase randomisation. Specifically, we can avoid using an additional ad-hoc module and focus rather on the working mechanism of the IM, which is part already of the transmitting unit. A common technique to modulate intensity is via a symmetric Mach–Zehnder interferometer (MZI). The light entering the MZI is first split into two beams and then recombined with a suitable phase. This will generate interference and therefore intensity modulation at the output ports of the MZI. By blocking one of the output ports, intensity modulation is obtained from the unblocked port as a result of the destructive or constructive interfering process. To modulate the relative phase between the two arms of the MZI, it is sufficient to control the refractive index of only one of the two MZI arms, and this is the most commonly used configuration. However, if a 'dual-drive' IM is used instead, both the arms in the MZI can be independently controlled, so to gain simultaneous control over the relative phase as well as the global phase of the signals traversing the IM respect to an external reference phase. If the global phase in the dual-drive IM is randomised, by encoding in each time slot a different phase value, Eve's probing signal will be phase randomised too and its phase will become uninformative to Eve. In this case, the state of the leaked signals seen by Eve will not be the one in equation (28) any more and will be replaced by the following one:

$$\rho_{\gamma_j} = \mathrm{e}^{-\beta^2_{\gamma_j}} \sum_{n=0}^{\infty} \frac{\beta^{2n}_{\gamma_j}}{n!} |n\rangle\langle n|. \tag{32}$$

We simulate the secure key rate for this situation using the detailed calculation of the trace distance terms $D_{n,j,k,l}$ given in appendix D.3 and setting the intensities $\beta^2_{\gamma_j}$ as in equation (31). That is, we still consider a THA where Eve's light crosses the IM first and is back-reflected to Eve from an interface placed after the IM in the transmitter architecture.

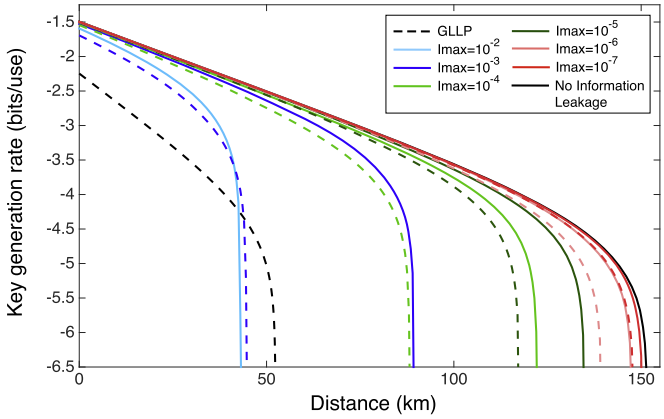

Figure 4. Secure key rate versus distance in presence of a THA targeting the modulating devices of a QKD transmitter. Each colour corresponds to a different value of the leaked intensity $I_{\max}$. The phase of the leaked light is randomised, see equation (32) in the main text. The solid lines are for a leakage due only to the IM while the dashed lines, corresponding to a much lower rate, are for the total leakage due to IM and PM simultaneously. For every distance, the key rate is maximised over the amplitudes γ_s and γ_v. All the parameters used in the simulation are listed in table 1.

The result of the simulation is reported in figure 4. It is apparent that the key rate has vastly improved with respect to figures 2 and 3. Even for a leakage intensity as large as $I_{\max} = 10^{-2}$, the key rate remains positive up to about 40 km. For an intensity smaller than $I_{\max} = 10^{-6}$, the resulting key rate is indistinguishable from the ideal one (solid black line) over almost the whole distance range. This shows the beneficial effect of phase randomisation, which was expected from the discussion in section 3.1.1. Differently from previous cases, the simultaneous information leakage from IM and PM (dashed lines in the figure) leads now to a key rate that is apparently lower than for a leakage due to the IM only (solid lines in the figure). For example, when $I_{\max} = 10^{-3}$ and the leakage is due to the IM only, the key rate remains positive for more than 85 km, while it falls below 50 km for a simultaneous leakage from PM and IM.

Given the benefit of phase randomisation, a natural question arises if sending only an n-photon Fock state, rather than its classical mixture, is beneficial to Eve. In appendix F, we discuss this point, and we show that the benefit of employing this attack Eve obtains is negligibly small, i.e., this attack can enlarge the trace distance only by the order of the transmission rate of Alice's device, which is negligible given the proper installation of optical isolators and filters. By recalling that phase randomisation transforms *any* state into a classical mixture of Fock states, we can conclude that the results presented in this section are essentially the secure key rate with the most general THA against IM assuming the phase randomisation.

From a practical perspective, phase randomisation makes the IM as robust against information leakage as a non-phase-randomised PM. This, in combination with the enhanced security due to the removal of any residual entanglement with Eve as well as that of all the off-diagonal elements, promotes phase randomisation as a relevant countermeasure to prevent the THA and the information leakage in general from the transmitter of decoy-state QKD and mdiQKD.

Before concluding this section, it is useful to summarise the physical models and the assumptions underlying our simulations. This is done with the help of figure 5.

In section 4.1, we considered the scenario depicted in figure 5(a), leading to equation (30). In this case, the coherent state of light back-reflected by the IM carries in its phase θ_{γ_j} the information about the intensity settings of the IM, γ_j. Its amplitude is the maximum allowed by any physical mechanism used to limit Eve's input light, irrespective of the IM settings, thus making the states outputted by Alice more distinguishable to Eve. This, together with the choice of the angles θ_{γ_j}, chosen to be most favourable to Eve, let us draw the worst-case key rate lines shown in figure 2.

In section 4.2, we devised a more realistic scenario, depicted in figure 5(b). Typically, Eve's light is reflected by an interface placed after the IM (double line in the figure) rather than by the IM itself. During the THA, Eve's light can pass through the IM when it is fully transmissive, to be reflected by the interface and pass through the IM again when the intensity settings are on. This way, Eve's light is modulated with exactly the same settings γ_j used by Alice for her own states, leading to equation (31) and figure 3.

Finally, in section 4.3, we applied phase randomisation to any light emerging from Alice's module, as shown in figure 5(c). For the intensity of the light back-reflected to Eve, we considered the same scenario as in figure 5(b). The ideal phase randomiser shown in the figure is a powerful resource as it removes any phase information from the output states, see equation (32), leading to better key rates, as reported in figure 4.

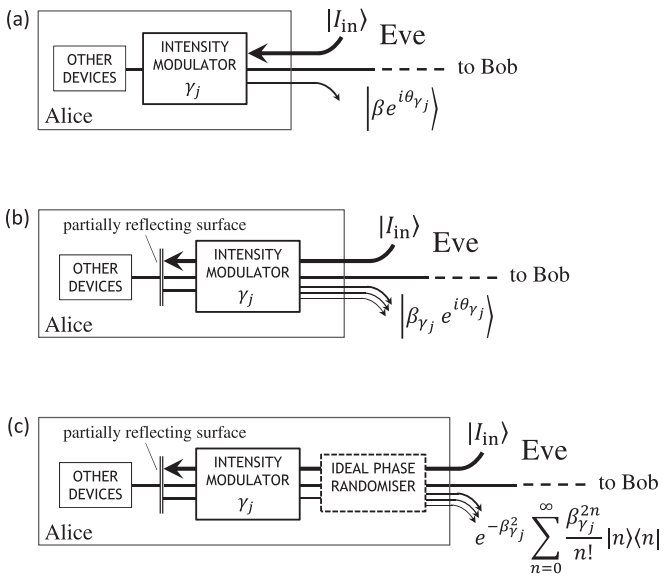

Figure 5. Models and states used in the simulation of individual THA targeting the IM. (a) The intensity of the back-reflected light is independent of the intensity settings (Case 1, section 4.1). (b) The intensity of the back-reflected light depends on the intensity settings (Case 2, section 4.2). (c) Eve's back-reflected light is phase randomised and it is represented by the classical mixture of Fock states (Case 3, section 4.3).

The model used to draw the lines for the PM is not explicitly described, as it is similar to the IM one and is detailed in [42]. Although the cases described in this section do not constitute an exhaustive list, they represent useful practical cases and can be used as guidelines for the secure implementation of real QKD systems.

5. Discussion

In this work, we have presented a general formalism to calculate the secret key rate of decoy-state QKD and mdiQKD under *any* THA directed against the transmitter's modulators. It is useful to give some insight into this formalism, in particular the one for IM, and discuss why the THA affects the standard theory of decoy states.

In the analysis of the decoy-state method without the THA, a fictitious protocol is considered where Alice delays her decision on the intensity settings after Bob detects a pulse. That is, after the detection of the pulse, Alice randomly decides the intensity setting $\gamma_{\rm s}$, $\gamma_{\rm v}$ and $\gamma_{\rm w}$ [30]. For simplicity, let us consider the discrimination between the signal state s and the first decoy state v only. By using the relation $\Pr(\gamma^i_{\rm s}|\text{click},\ n) + \Pr(\gamma^i_{\rm v}|\text{click},\ n) = 1$ and the Bayes's rule, we can rewrite equation (4) as:

$$\left| \frac{\Pr(\gamma_{\rm v})}{\Pr(\gamma_{\rm s}) + \Pr(\gamma_{\rm v})} - \Pr(\gamma^i_{\rm v}|\text{click},\ n) \right| \leqslant \frac{\Pr(\gamma_{\rm s})\Pr(\gamma_{\rm v})}{\Pr(\gamma_{\rm s}) + \Pr(\gamma_{\rm v})} \frac{\overline{D}_{n,{\rm s},{\rm v}}}{\Pr^i(\text{click}|n)}, \tag{33}$$

where $\overline{D}_{n,{\rm s},{\rm v}} := \max_i D^i_{n,{\rm s},{\rm v}}$. From this equation, we see that in the case of no THA, $\overline{D}_{n,{\rm s},{\rm v}} = 0$ and $\frac{\Pr(\gamma_{\rm v})}{\Pr(\gamma_{\rm s}) + \Pr(\gamma_{\rm v})} = \Pr(\gamma^i_{\rm v}|\text{click},\ n)$ for any i and n. This entails that Alice's assignment of the intensities in the fictitious protocol can be made identical and independent of the instance i over the detected instances. This allows us to use probability inequalities, such as the multiplicative chernoff bound [30], which applies to independent trials. However, when the THA is on the line, $\overline{D}_{n,{\rm s},{\rm v}} \neq 0$ and the bound to the lhs of equation (33) becomes dependent on the instance i. To solve this problem, we make use of Azuma's inequality [56]. Because we are in the asymptotic scenario, the technical details related to the inequality are unnecessary and we will not write them here explicitly.

Our formalism does not require any knowledge of Eve's measurement for the THA or the detailed specification of the state used. Instead, a detailed characterisation of the modulators is needed. This is important because while the full characterisation of Alice's modulators over many modes is doable at least in principle, the characterisation of Eve's THA is impossible even in principle. However, the full characterisation of Alice's modulators might be challenging in practice and further research needs to be done in this direction. We remark that our formalism is a powerful tool in this context because it can readily accept any mathematical model that describes the behaviour of the modulators.

As we have discussed in section 3.1.1 and practically demonstrated in section 4.3, it is important to perform phase randomisation of Eve's signals to defeat the THA exploiting entanglement and to enhance the key rate.

However, on the other hand, it is important to perform the randomisation without opening additional loopholes. Also, the question remains of whether this solution is more practical than the one based on a series of optical isolators. Active phase randomisation requires precise synchronisation and a sequence of random numbers in the input. Even if correctly performed, a certain level of optical isolation is always needed to shield a system from the external environment. The total amount of required isolation clearly depends on phase randomisation, as seen by comparing figures 3 and 4. However, these figures also show that the difference in the values of $I_{\max}$ amounts roughly to 60 dB, which can be achieved with a single entirely passive component like a dual-stage optical isolator. Hence even high isolation levels can be inexpensively achieved through a series of such isolators.

6. Conclusion

In this paper, we have quantified the secure key rate of decoy-state-based QKD in presence of leaky transmitters. This allowed us to suggest quantitative countermeasures to restore security even in this more general scenario. A real setup is typically leaky in practice, due to the presence of side channels hidden in the preparation of the communication signals, or due to the active intervention of an eavesdropper. The analysis of this case is then of immediate practical interest. Our analysis applies to any decoy-state system that uses an IM or a PM to distill a quantum key. It includes in fact the most general attack based on the extra information possibly leaked from such devices.

We have employed our formalism to analyse particular examples of THA, where Eve exploits coherent states of light to probe the intensity and PM in the transmitter. Our results show that it is possible to distill a key from leaky transmitters that approach the ideal rate of a perfectly shielded system. For that, two main solutions play a crucial role. On one hand, optical isolation has to be guaranteed for any system through an adequate number of attenuators and optical isolators. On the other hand, active phase randomisation can further enhance the protection, removing any residual entanglement from Eve's probing signals.

Given the generality of our approach and its applicability to cases of practical interest, we believe that it will become a fundamental tool to analyse the security of real-world quantum communication systems, including those for standard QKD, mdiQKD and the device-independent QKD where PM and/or IM are used.

Acknowledgments

The authors wish to thank Norbert Lütkenhaus for very useful discussions, and the anonymous referees for their constructive comments which have helped us to significantly improve of this paper. This work was supported by the Galician Regional Government (program 'Ayudas para proyectos de investigación desarrollados por investigadores emergentes' EM2014/033, and consolidation of Research Units: AtlantTIC), the Spanish Ministry of Economy and Competitiveness (MINECO), the Fondo Europeo de Desarrollo Regional (FEDER) through grant TEC2014-54898-R, the ImPACT Program of the Council for Science, Technology and Innovation (Cabinet Office, Government of Japan), and the project EMPIR 14IND05 MIQC2. This project has received funding from the EMPIR programme co-financed by the Participating States and from the European Unions Horizon 2020 research and innovation programme.

Appendix A. Azuma's inequality

In this appendix we introduce Azuma's inequality [56]. It can be applied to a sequence of random variables $X^{(0)}, X^{(1)}, \ldots, X^{(l)}$ that satisfies the martingale and the bounded difference conditions (BDC). In particular, a set of random variables is called a martingale if and only if $E[X^{(l+1)}|X^{(0)}, X^{(1)}, \ldots, X^{(l)}] = X^{(l)}$ holds for any l, where $E[\cdot]$ represents the expectation value. That is, the expectation value of the $(l+1)$th random variable conditional on all the previous random variables is equal to the lth random variable. On the other hand, $X^{(0)}, X^{(1)}, \ldots, X^{(l)}$ satisfies the BDC if and only if there exists $c^{(l)} > 0$ such that $|X^{(l+1)} - X^{(l)}| \leqslant c^{(l)}$ for any l. In this scenario, Azuma's inequality states that

$$\Pr[|X^{(l)} - X^{(0)}| > l\delta] \leqslant 2e^{-\frac{l^2\delta^2}{2\sum_{k=1}^{l}(c^{(l)})^2}} \tag{A.1}$$

for any $\delta \in (0, 1)$.

Now, to derive the result that we use in the main text, we proceed as follows. In particular, let us consider that we flip coins starting from the first coin in order. The coins can be correlated in an arbitrary manner. Let y_u be the random variable that represents the result of the uth coin, with $y_u = 1$ when the result is head and $y_u = 0$ when it is tail. Let $P(y_u = 1|\xi_0, \ldots, \xi_{u-1})$ be the conditional probability of having head in the uth coin conditional on all the results of the previous coins, which we denote as $\xi_0, \ldots, \xi_{u-1}$. Finally, we denote by $\Lambda^{(l)}$ the actual number of heads obtained after flipping l coins. Then, it can be shown that

$$X^{(l)} := \Lambda^{(l)} - \sum_{u=1}^{l} P(y_u = 1|\xi_0, \ldots, \xi_{u-1}) \tag{A.2}$$

is a martingale and satisfies the BDC We have, therefore, that

$$\Pr[|\Lambda^{(N)} - \sum_{u=1}^{N} P(y_u = 1|\xi_0, \ldots, \xi_{u-1})| > N\delta] \leqslant 2e^{-\frac{N\delta^2}{2}}. \tag{A.3}$$

Appendix B. Joint THA when the IM and the PM are correlated

In this appendix, we explain briefly how to adapt our formalism to evaluate the situation where there are arbitrary correlations between the IM and the PM, and Eve can exploit this fact in her THA.

In this correlated scenario, Alice and Bob could first estimate the bit and basis dependent single-photon yield, which we denote as $Y_1^{\gamma_s,\xi_A,\zeta_A}$, for the signal setting. Here, the parameter ξ_A denotes Alice's bit value and ζ_A is her basis choice. That is, $Y_1^{\gamma_s,\xi_A,\zeta_A}$ represents the conditional probability that Bob obtains a 'click' event given that Alice selects the signal setting and sends him a single-photon state encoding a bit value ξ_A in the basis ζ_A. To estimate this yield, Alice can declare Bob (over the authenticated public channel) all the bit and basis information associated to those instances where she used a decoy setting and Bob obtained a 'click' event. With this information, Alice and Bob can estimate $Y_1^{\gamma_s,\xi_A,\zeta_A}$ by using a modified version of equation (6) given by

$$|Y_n^{\gamma_j,\xi_A,\zeta_A} - [q_{nkl} Y_n^{\gamma_k,\xi_A,\zeta_A} + (1 - q_{nkl}) Y_n^{\gamma_l,\xi_A,\zeta_A}]| \leqslant D_{n,j,k,l}^{\xi_A,\zeta_A}. \tag{B.1}$$

Here, the parameter $D_{n,j,k,l}^{\xi_A,\zeta_A}$ is a modified version of $D_{n,j,k,l}$ that refers solely to the set of choices $\{\xi_A, \zeta_A\}$. Note that this modification is needed because now the decoy-state method is bit-and-basis-dependent. With a procedure similar to the one adopted to go from equation (6) to equation (8), one can obtain the single-photon bit error rate for the signal setting, which also depends on Bob's basis choice and on his bit value.

After obtaining the single-photon yield as well as the associated error rate, Alice and Bob generate a secret key from those instances where Alice emitted a single-photon pulse prepared in the Z basis and using the signal setting, and Bob obtained a 'click' event when he measured the pulse in the Z basis. Note that all the statistics associated to such instances are estimated through the bit-and-basis-dependent decoy-state method. Likewise, one can readily obtain the single-photon yield associated to those events where Alice emits a single-photon pulse prepared in the X basis and using the signal setting, and Bob obtains a 'click' event when he uses the X basis. Now, to generate a key, one follows the technique explained in section 3.2 except for a small modification. One has to replace $\hat{U}_{A_p,A_a,E_p}^{\zeta,i}$ in equation (22) with $\hat{U}_{A_p,A_a,E_p}^{\zeta,i,\gamma_s,1}$, which is a restricted version of $\hat{U}_{A_p,A_a,E_p}^{\zeta,i}$ that only considers the single-photon emission part in the signal setting. That is, Alice and Bob have to characterise the behaviour of the PM depending on their bases choice when they select the signal setting.

With the modifications above, one can obtain the phase error rate $\delta_{X-\text{Error}|Z}$ from equation (26) because the bit-and-basis-dependent decoy-state method allows us to evaluate all the parameters needed to solve this equation, all of which are now restricted only to the single-photon emission events. Then, in the asymptotic limit of a large number of transmitted signals, we have that the secure key rate is given by

$$K \geqslant \sum_{i=0}^{1} q \{p_0^{\gamma_s,i,Z} Y_{0L}^{\gamma_s,i,Z} + p_1^{\gamma_s,i,Z} Y_{1L}^{\gamma_s,i,Z} [1 - h(\delta_{X-\text{Error}|Z})] - f(E^{\gamma_s}) Q^{\gamma_s} h(E^{\gamma_s})\}, \tag{B.2}$$

where $p_0^{\gamma_s,i,Z}$ is the probability that Alice emits the vacuum state given that she chooses γ_s and the bit value i in the Z basis. The other parameters which appear in equation (B.2) are defined in a similar manner (see also equation (29)). Therefore, we conclude that one can apply our formalism to analyse also the case where there are arbitrary correlations between the IM and the PM, and prove security in the most general case, given that a full description of the behaviour of these two devices is available.

Appendix C. Estimation of $Y_{0L}^{\gamma_s}$, $Y_{1L}^{\gamma_s}$ and $e_{1U}^{\gamma_s}$

In this appendix we show that these parameters can be estimated using linear programming. Such instances of optimisation problems can be solved efficiently in polynomial time [66]. Although the estimation method presented here is valid for any number of decoy states used by Alice, we will assume, like in the main text, that Alice employs three different intensity settings: γ_s, γ_v and γ_w.

Our starting point is equation (6). Let us consider first the case $k = l$. As shown in appendix D, the parameters $D_{n,j,k}$ do not depend on the photon number n, at least for the examples considered in section 4. This means, in particular, that this equation can be rewritten as

$$|Y_n^{\gamma_j} - Y_n^{\gamma_k}| \leqslant D_{j,k}, \tag{C.1}$$

or, equivalently, the yields $Y_n^{\gamma_j}$ and $Y_n^{\gamma_k}$ satisfy

$$Y_n^{\gamma_j} = Y_n^{\gamma_k} + \Delta^{jk}, \tag{C.2}$$

with $\Delta^{jk} \in [-D_{j,k}, D_{j,k}]$. Since Alice uses three different intensity settings, we have the following six conditions

$$\begin{aligned} Y_n^{\gamma_s} &= Y_n^{\gamma_v} + \Delta^{sv}, & Y_n^{\gamma_s} &= Y_n^{\gamma_w} + \Delta^{sw}, \\ Y_n^{\gamma_v} &= Y_n^{\gamma_s} + \Delta^{vs}, & Y_n^{\gamma_v} &= Y_n^{\gamma_w} + \Delta^{vw}, \\ Y_n^{\gamma_w} &= Y_n^{\gamma_s} + \Delta^{ws}, & Y_n^{\gamma_w} &= Y_n^{\gamma_v} + \Delta^{wv}. \end{aligned} \tag{C.3}$$

By combining the first and the third one, we find, for example, that $\Delta^{sv} = -\Delta^{vs}$. Similarly, we obtain $\Delta^{sw} = -\Delta^{ws}$ and $\Delta^{vs} - \Delta^{ws} = \Delta^{vw} = -\Delta^{wv}$. By using this last condition we find, therefore, that

$$\begin{aligned} Y_n^{\gamma_v} &= Y_n^{\gamma_s} + \Delta^{vs} = Y_n^{\gamma_s} + \Delta^{ws} + \Delta^{vw}, \\ Y_n^{\gamma_w} &= Y_n^{\gamma_s} + \Delta^{ws}. \end{aligned} \tag{C.4}$$

That is, we can express the yields $Y_n^{\gamma_v}$ and $Y_n^{\gamma_w}$ as a function of $Y_n^{\gamma_s}$ and the parameters Δ^{ws} and Δ^{vw}.

Next, we consider the case $k \neq l$. In this scenario, equation (6) can be rewritten as

$$Y_n^{\gamma_j} = q_{nkl} Y_n^{\gamma_k} + (1 - q_{nkl}) Y_n^{\gamma_l} + \Delta^{njkl}, \tag{C.5}$$

for all n, where $\Delta^{njkl} \in [-D_{n,j,k,l}, D_{n,j,k,l}]$. We have, therefore, the following three conditions:

$$\begin{aligned} Y_n^{\gamma_s} &= q_{nvw} Y_n^{\gamma_v} + (1 - q_{nvw}) Y_n^{\gamma_w} + \Delta^{nsvw}, \\ Y_n^{\gamma_v} &= q_{nsw} Y_n^{\gamma_s} + (1 - q_{nsw}) Y_n^{\gamma_w} + \Delta^{nvsw}, \\ Y_n^{\gamma_w} &= q_{nsv} Y_n^{\gamma_s} + (1 - q_{nsv}) Y_n^{\gamma_v} + \Delta^{nwsv}. \end{aligned} \tag{C.6}$$

If we substitute in these equations the value of $Y_n^{\gamma_v}$ and $Y_n^{\gamma_w}$ given by equation (C.4) we obtain the following three equality constraints:

$$\begin{aligned} 0 &= \Delta^{ws} + q_{nvw} \Delta^{vw} + \Delta^{nsvw}, \\ 0 &= q_{nsw} \Delta^{ws} + \Delta^{vw} - \Delta^{nvsw}, \\ 0 &= q_{nsv} \Delta^{ws} - (1 - q_{nsv}) \Delta^{vw} - \Delta^{nwsv}. \end{aligned} \tag{C.7}$$

Finally, by taking into account that $\Delta^{njkl} \in [-D_{n,j,k,l}, D_{n,j,k,l}]$ for all n and for all $j, k, l \in \{s, v, w\}$ with $j \neq k \neq l$, we have that to satisfy equation (C.7) we must fulfill the following conditions:

$$\begin{aligned} -D_{n,s,v,w} &\leqslant \Delta^{ws} + q_{nvw} \Delta^{vw} \leqslant D_{n,s,v,w}, \\ -D_{n,v,s,w} &\leqslant q_{nsw} \Delta^{ws} + \Delta^{vw} \leqslant D_{n,v,s,w}, \\ -D_{n,w,s,v} &\leqslant q_{nsv} \Delta^{ws} - (1 - q_{nsv}) \Delta^{vw} \leqslant D_{n,w,s,v}. \end{aligned} \tag{C.8}$$

C.1. Estimation of $Y_{0L}^{\gamma_s}$

Here we present a linear program to estimate the parameter $Y_{0L}^{\gamma_s}$. We will assume that all the quantities below refer to events where both Alice and Bob use the same basis (e.g., the Z basis), which will be considered as the key generation basis. We start by calculating the gain associated to the different intensity settings selected by Alice in this scenario. If we combine equations (2) and (C.4) we have that

$$\begin{aligned} Q^{\gamma_s} &= \sum_{n=0}^{\infty} p_n^{\gamma_s} Y_n^{\gamma_s}, \\ Q^{\gamma_v} &= \sum_{n=0}^{\infty} p_n^{\gamma_v} (Y_n^{\gamma_s} + \Delta^{ws} + \Delta^{vw}) = \sum_{n=0}^{\infty} p_n^{\gamma_v} Y_n^{\gamma_s} + \Delta^{ws} + \Delta^{vw}, \\ Q^{\gamma_w} &= \sum_{n=0}^{\infty} p_n^{\gamma_w} (Y_n^{\gamma_s} + \Delta^{ws}) = \sum_{n=0}^{\infty} p_n^{\gamma_w} Y_n^{\gamma_s} + \Delta^{ws}. \end{aligned} \tag{C.9}$$

That is, all the gains can be written as a function of the yields $Y_n^{\gamma_s}$ together with the additional terms Δ^{ws} and Δ^{vw}.

Equation (C.9) contains an infinite number of unknown parameters $Y_n^{\gamma_s}$. Next, we reduce it to a finite set. For this, we derive a lower and upper bound for the gains Q^{γ} that only depend on a finite number, $S_{\text{cut}} + 1$, of yields $Y_n^{\gamma_s}$. In particular, since $0 \leqslant Y_n^{\gamma_s} \leqslant 1$ and $p_n^{\gamma_s} \geqslant 0$ for all n, we have that

$$Q^{\gamma_s} \geqslant \sum_{n=0}^{S_{\rm cut}} p_n^{\gamma_s} Y_n^{\gamma_s},$$
$$Q^{\gamma_s} \leqslant \sum_{n=0}^{S_{\rm cut}} p_n^{\gamma_s} Y_n^{\gamma_s} + \sum_{n=S_{\rm cut}+1}^{\infty} p_n^{\gamma_s} = \sum_{n=0}^{S_{\rm cut}} p_n^{\gamma_s} Y_n^{\gamma_s} + \Gamma^{\gamma_s}, \tag{C.10}$$

for any $S_{\rm cut} \geqslant 0$. Here the parameter Γ^{γ_s} is defined as $\Gamma^{\gamma_s} = \sum_{n=S_{\rm cut}+1}^{\infty} p_n^{\gamma_s} = 1 - \sum_{n=0}^{S_{\rm cut}} p_n^{\gamma_s}$. By using a similar procedure, one can obtain as well a lower and upper bound for Q^{γ_v} and Q^{γ_w}.

Based on the foregoing, we find that $Y_{0\rm L}^{\gamma_s}$ can be calculated using the following linear program:

$$\begin{aligned}
\min \quad & Y_0^{\gamma_s} \\
\text{s. t.} \quad & Q^{\gamma_s} \geqslant \sum_{n=0}^{S_{\rm cut}} p_n^{\gamma_s} Y_n^{\gamma_s}, \\
& Q^{\gamma_s} - \Gamma^{\gamma_s} \leqslant \sum_{n=0}^{S_{\rm cut}} p_n^{\gamma_s} Y_n^{\gamma_s}, \\
& Q^{\gamma_v} \geqslant \sum_{n=0}^{S_{\rm cut}} p_n^{\gamma_v} Y_n^{\gamma_s} + \Delta^{\rm ws} + \Delta^{\rm vw}, \\
& Q^{\gamma_v} - \Gamma^{\gamma_v} \leqslant \sum_{n=0}^{S_{\rm cut}} p_n^{\gamma_v} Y_n^{\gamma_s} + \Delta^{\rm ws} + \Delta^{\rm vw}, \\
& Q^{\gamma_w} \geqslant \sum_{n=0}^{S_{\rm cut}} p_n^{\gamma_w} Y_n^{\gamma_s} + \Delta^{\rm ws}, \\
& Q^{\gamma_w} - \Gamma^{\gamma_w} \leqslant \sum_{n=0}^{S_{\rm cut}} p_n^{\gamma_w} Y_n^{\gamma_s} + \Delta^{\rm ws}, \\
& 0 \leqslant Y_n^{\gamma_s} \leqslant 1, \ \forall n \leqslant S_{\rm cut}, \\
& -D_{\rm w,s} \leqslant \Delta^{\rm ws} \leqslant D_{\rm w,s}, \quad -D_{\rm v,w} \leqslant \Delta^{\rm vw} \leqslant D_{\rm v,w}, \\
& -D_{n,\rm s,v,w} \leqslant \Delta^{\rm ws} + q_{n\rm vw}\Delta^{\rm vw} \leqslant D_{n,\rm s,v,w}, \ \forall n \leqslant S_{\rm cut}, \\
& -D_{n,\rm v,s,w} \leqslant q_{n\rm sw}\Delta^{\rm ws} + \Delta^{\rm vw} \leqslant D_{n,\rm v,s,w}, \ \forall n \leqslant S_{\rm cut}, \\
& -D_{n,\rm w,s,v} \leqslant q_{n\rm sv}\Delta^{\rm ws} - (1 - q_{n\rm sv})\Delta^{\rm vw} \leqslant D_{n,\rm w,s,v}, \ \forall n \leqslant S_{\rm cut}.
\end{aligned} \tag{C.11}$$

Note that the value of the parameters $D_{j,k}$ and $D_{n,j,k,l}$, with $j, k, l \in \{\rm s, v, w\}$, is provided in appendix D. Also, the value of the observables Q^{γ_j} for a typical channel model can be found in appendix E. The linear program above has $S_{\rm cut} + 3$ unknown parameters: $Y_n^{\gamma_s}$, $\Delta^{\rm ws}$ and $\Delta^{\rm vw}$. Its solution is directly $Y_{0\rm L}^{\gamma_s}$.

C.2. Estimation of $Y_{1\rm L}^{\gamma_s}$

To calculate $Y_{1\rm L}^{\gamma_s}$, we can reuse the linear program given by equation (C.11), only substituting its linear objective function with $Y_1^{\gamma_s}$.

C.3. Estimation of $e_{1\rm U}^{\gamma_s}$

To obtain $e_{1\rm U}^{\gamma_s}$, we can again reuse the linear program given by equation (C.11), only making the following three changes. First, all the parameters now refer to the X basis rather than the Z basis. For example, Q^{γ_j} now denotes the gain when Alice selects the intensity setting γ_j and both Alice and Bob use the X basis, and similarly for the other quantities that appear in equation (C.11). Second, we substitute the parameters Q^{γ_j} with $Q^{\gamma_j}E^{\gamma_j}$ for all $j \in \{\rm s, v, w\}$, and we replace the yields $Y_n^{\gamma_s}$ with other variables that we will denote as $\omega_n^{\gamma_s}$. These variables represent the value of $Y_n^{\gamma_s} e_n^{\gamma_s}$. Third, we substitute the linear objective function with $-\omega_1^{\gamma_s}$, where the minus sign is because equation (C.11) is a minimisation problem and we are interested in obtaining an upper bound for $\omega_1^{\gamma_s}$.

If we denote the solution to this optimisation problem as $n_{\rm sol}$, then $e_{1\rm U}^{\gamma_s}$ is simply given by

$$e_{1\rm U}^{\gamma_s} = -\frac{n_{\rm sol}}{Y_{1\rm L}^{\gamma_s}}, \tag{C.12}$$

where, again, $Y_{1\rm L}^{\gamma_s}$ now denotes a lower bound on the yield of the single-photon pulses when both Alice and Bob employ the X basis. The value of the observables Q^{γ_j} and E^{γ_j} for a typical channel model is provided in appendix E.

Appendix D. Estimation of $D_{n,j,k}$ and $D_{n,j,k,l}$

In this appendix we calculate the parameters $D_{n,j,k}$ and $D_{n,j,k,l}$ for the three examples studied in section 4. These parameters are needed to estimate a lower bound on the yields $Y_0^{\gamma_s}$ and $Y_1^{\gamma_s}$, together with an upper bound on the phase error rate $e_1^{\gamma_s}$, which is done in appendix C.

All these examples correspond to individual THA, which implies that the states ρ_{n,γ_j^i}, which are accessible to Eve, do not depend on the instance i. In addition, they assume, as expected in most practical situations, that there is no correlation between Alice's system A_p and Eve's system E'_p. That is, $\rho_{n,\gamma_j^i} = \hat{P}(|n\rangle) \otimes \rho_{\gamma_j}$. This means, in particular, that

$$\begin{aligned} D_{n,j,k} &= d(\rho_{\gamma_j}, \rho_{\gamma_k}), \\ D_{n,j,k,l} &= d(\rho_{\gamma_j}, q_{nkl}\rho_{\gamma_k} + (1 - q_{nkl})\rho_{\gamma_l}), \end{aligned} \tag{D.1}$$

for all n. In this scenario, the parameters $D_{n,j,k}$ do not depend on the photon number n and we will denote them as $D_{j,k}$. Next, we calculate these quantities for the different cases.

D.1. Individual THA—Case 1

In this example, the states ρ_{γ_j} are of the form $\rho_{\gamma_j} = \hat{P}(|\beta e^{i\theta_{\gamma_j}}\rangle)$. We have, therefore, that

$$D_{j,k} = \sqrt{1 - |\langle \beta e^{i\theta_{\gamma_j}}|\ \beta e^{i\theta_{\gamma_k}}\rangle|^2} = \sqrt{1 - e^{2\beta^2[\cos(\theta_{\gamma_k} - \theta_{\gamma_j}) - 1]}}. \tag{D.2}$$

Here we can assume, without loss of generality, that $\theta_{\gamma_s} = 0$. Moreover, we will denote $\beta^2 := I_{\max}$. This implies, in particular, that $D_{w,s}$ and $D_{v,w}$ are given by

$$\begin{aligned} D_{w,s} &= \sqrt{1 - e^{2I_{\max}[\cos(\theta_{\gamma_w}) - 1]}}, \\ D_{v,w} &= \sqrt{1 - e^{2I_{\max}[\cos(\theta_{\gamma_w} - \theta_{\gamma_v}) - 1]}}. \end{aligned} \tag{D.3}$$

The parameters $D_{n,j,k,l}$ have the form

$$D_{n,j,k,l} = \frac{1}{2}\,|\hat{P}(|\beta e^{i\theta_{\gamma_j}}\rangle) - q_{nkl}\hat{P}(|\beta e^{i\theta_{\gamma_k}}\rangle) - (1 - q_{nkl})\hat{P}(|\beta e^{i\theta_{\gamma_l}}\rangle)|. \tag{D.4}$$

In order to calculate these quantities we use the following Claim, which requires to obtain the eigenvalues of a 3×3 matrix.

Claim. *Let* $\{|\alpha\rangle_i\}_{i=\{1,2,3\}}$, be three normalised but not necessarily orthogonal vectors, and let λ_i be the eigenvalues of a 3×3 matrix A defined as

$$(A)_{i,j} = \delta_{i,1}\langle\alpha_1|\ \alpha_j\rangle - p\delta_{i,2}\langle\alpha_2|\ \alpha_j\rangle - (1 - p)\delta_{i,3}\langle\alpha_3|\ \alpha_j\rangle, \tag{D.5}$$

with $1 \geqslant p \geqslant 0$ and where $\delta_{i,j}$ is the Kronecker delta. Then

$$\frac{1}{2}\,|\hat{P}(|\alpha_1\rangle) - p\hat{P}(|\alpha_2\rangle) - (1 - p)\hat{P}(|\alpha_3\rangle)| = \frac{1}{2}\sum_i |\lambda_i|. \tag{D.6}$$

Proof. To calculate the trace distance of $\rho := \hat{P}(|\alpha_1\rangle) - p\hat{P}(|\alpha_2\rangle) - (1 - p)\hat{P}(|\alpha_3\rangle)$ we need to determine its eigenvalues. Moreover, from the properties of the determinant we have that $\mathrm{Det}(\rho - \lambda\hat{\mathbb{1}}) = \mathrm{Det}(V^{-1}\rho V - \lambda\hat{\mathbb{1}})$ for any invertible linear operation V. Then, we can construct V as follows

$$V\,|i\rangle = |\alpha_i\rangle, \qquad \text{and} \qquad \langle i|\ V^{-1} = \langle\bar{\alpha}_i|, \tag{D.7}$$

where $\{|i\rangle\}_{i=\{1,2,3\}}$ is an orthonormal basis, and $|\bar{\alpha}_i\rangle$ represent unnormalised vectors satisfying $\langle\bar{\alpha}_i|\ \alpha_j\rangle = \delta_{i,j}$. With these definitions, we can use V and $|\bar{\alpha}_i\rangle$ to relate the matrix elements of $V^{-1}\rho V$ defined in the orthogonal basis $\{|i\rangle\}_i$ to those of ρ defined in the nonorthogonal basis $\{|\alpha_i\rangle\}_i$. In particular, we have that

$$\begin{aligned} \langle i|\ V^{-1}\rho V\,|j\rangle = \langle\bar{\alpha}_i|\ \rho\ |\alpha_j\rangle &= \langle\bar{\alpha}_i|\ \hat{P}(|\alpha_1\rangle)|\alpha_j\rangle - p\langle\bar{\alpha}_i|\ \hat{P}(|\alpha_2\rangle)|\alpha_j\rangle \\ &\quad - (1 - p)\langle\bar{\alpha}_i|\ \hat{P}(|\alpha_3\rangle)|\alpha_j\rangle = (A)_{i,j}, \end{aligned} \tag{D.8}$$

with $(A)_{i,j}$ given by equation (D.5).

D.2. Individual THA—Case 2

In this example, the states ρ_{γ_j} are of the form $\rho_{\gamma_j} = \hat{P}(|\beta_{\gamma_j} e^{i\theta_{\gamma_j}}\rangle)$, where the amplitudes β_{γ_j} are given in equation (31). That is, here we assume that the back-reflected light that goes to Eve is attenuated in a similar manner as Alice's signals. In this scenario, we have that

$$\begin{aligned} D_{j,k} &= \sqrt{1 - |\langle\beta_{\gamma_j} e^{i\theta_{\gamma_j}}|\ \beta_{\gamma_k} e^{i\theta_{\gamma_k}}\rangle|^2} \\ &= \sqrt{1 - e^{-\beta_{\gamma_j}^2 - \beta_{\gamma_k}^2 + 2\beta_{\gamma_j}\beta_{\gamma_k}\cos(\theta_{\gamma_k} - \theta_{\gamma_j})}}. \end{aligned} \tag{D.9}$$

Again, if we assume, without loss of generality, that $\theta_{\gamma_s} = 0$ and we use equation (31) we find that the quantities $D_{w,s}$ and $D_{v,w}$ are given by

$$D_{\mathrm{w,s}} = \sqrt{1 - \mathrm{e}^{-\frac{I_{\max}}{\gamma_{\mathrm{s}}}[\gamma_{\mathrm{s}}+\gamma_{\mathrm{w}}-2\sqrt{\gamma_{\mathrm{s}}\gamma_{\mathrm{w}}}\cos(\theta_{\gamma_{\mathrm{w}}})]}},$$
$$D_{\mathrm{v,w}} = \sqrt{1 - \mathrm{e}^{-\frac{I_{\max}}{\gamma_{\mathrm{s}}}[\gamma_{\mathrm{v}}+\gamma_{\mathrm{w}}-2\sqrt{\gamma_{\mathrm{v}}\gamma_{\mathrm{w}}}\cos(\theta_{\gamma_{\mathrm{w}}}-\theta_{\gamma_{\mathrm{v}}})]}}. \tag{D.10}$$

The parameters $D_{n,j,k,l}$ have the form

$$D_{n,j,k,l} = \frac{1}{2}\,|\hat{P}(|\beta_{\gamma_j}\mathrm{e}^{\mathrm{i}\theta_{\gamma_j}}\rangle) - q_{nkl}\hat{P}(|\beta_{\gamma_k}\mathrm{e}^{\mathrm{i}\theta_{\gamma_k}}\rangle) - (1-q_{nkl})\hat{P}(|\beta_{\gamma_l}\mathrm{e}^{\mathrm{i}\theta_{\gamma_l}}\rangle)|. \tag{D.11}$$

Like in the previous subsection, we calculate these quantities by using the Claim introduced above.

D.3. Individual THA—Case 3

Here the states ρ_{γ_j} are of the form given by equation (32) with the intensities $\beta^2_{\gamma_j}$ given by equation (31). This corresponds to the scenario where Eve's back-reflected light is phase-randomised and, moreover, it is attenuated in a similar manner as Alice's signals. In this situation, we have that

$$D_{j,k} = \frac{1}{2}\sum_{n=0}^{\infty}\left|\mathrm{e}^{-\beta^2_{\gamma_j}}\frac{\beta^{2n}_{\gamma_j}}{n!} - \mathrm{e}^{-\beta^2_{\gamma_k}}\frac{\beta^{2n}_{\gamma_k}}{n!}\right|. \tag{D.12}$$

This means, in particular, that the parameters $D_{\mathrm{w,s}}$ and $D_{\mathrm{v,w}}$ are given by

$$D_{\mathrm{w,s}} = \frac{\mathrm{e}^{-I_{\max}}}{2}\sum_{n=0}^{\infty}\frac{I^n_{\max}}{n!}\left|1 - \mathrm{e}^{I_{\max}(1-\gamma_{\mathrm{w}}/\gamma_{\mathrm{s}})}\left(\frac{\gamma_{\mathrm{w}}}{\gamma_{\mathrm{s}}}\right)^n\right|,$$
$$D_{\mathrm{v,w}} = \frac{1}{2}\mathrm{e}^{-\frac{I_{\max}\gamma_{\mathrm{v}}}{\gamma_{\mathrm{s}}}}\sum_{n=0}^{\infty}\frac{(I_{\max}\gamma_{\mathrm{v}}/\gamma_{\mathrm{s}})^n}{n!}\left|1 - \mathrm{e}^{I_{\max}\gamma_{\mathrm{v}}/\gamma_{\mathrm{s}}(1-\gamma_{\mathrm{w}}/\gamma_{\mathrm{v}})}\left(\frac{\gamma_{\mathrm{w}}}{\gamma_{\mathrm{v}}}\right)^n\right|. \tag{D.13}$$

These expressions involve an infinite number of terms. However, one can easily upper bound them with a finite sum. For instance, it can be shown that when $I_{\max} \leqslant \log 2$ and $\gamma_{\mathrm{s}} \geqslant \gamma_{\mathrm{v}} \geqslant \gamma_{\mathrm{w}}$ (which is always satisfied in the simulation results shown in section 4) $D_{\mathrm{w,s}}$ and $D_{\mathrm{v,w}}$ can be upper bounded as

$$D_{\mathrm{w,s}} \leqslant \frac{1}{2} - \frac{\mathrm{e}^{-I_{\max}}}{2}\sum_{n=0}^{P_{\mathrm{cut}}}\frac{I^n_{\max}}{n!}\left[1 - \left|1 - \mathrm{e}^{I_{\max}(1-\gamma_{\mathrm{w}}/\gamma_{\mathrm{s}})}\left(\frac{\gamma_{\mathrm{w}}}{\gamma_{\mathrm{s}}}\right)^n\right|\right],$$
$$D_{\mathrm{v,w}} \leqslant \frac{1}{2} - \frac{1}{2}\mathrm{e}^{-\frac{I_{\max}\gamma_{\mathrm{v}}}{\gamma_{\mathrm{s}}}}\sum_{n=0}^{P_{\mathrm{cut}}}\frac{(I_{\max}\gamma_{\mathrm{v}}/\gamma_{\mathrm{s}})^n}{n!} \times\left[1 - \left|1 - \mathrm{e}^{I_{\max}\gamma_{\mathrm{v}}/\gamma_{\mathrm{s}}(1-\gamma_{\mathrm{w}}/\gamma_{\mathrm{v}})}\left(\frac{\gamma_{\mathrm{w}}}{\gamma_{\mathrm{v}}}\right)^n\right|\right]. \tag{D.14}$$

for any $P_{\mathrm{cut}} \geqslant 1$. To see this, let us consider, for instance, the parameter $D_{\mathrm{w,s}}$. From equation (D.13) we have that $D_{\mathrm{w,s}}$ satisfies

$$D_{\mathrm{w,s}} = \frac{\mathrm{e}^{-I_{\max}}}{2}\sum_{n=0}^{P_{\mathrm{cut}}}\frac{I^n_{\max}}{n!}\left|1 - \mathrm{e}^{I_{\max}(1-\gamma_{\mathrm{w}}/\gamma_{\mathrm{s}})}\left(\frac{\gamma_{\mathrm{w}}}{\gamma_{\mathrm{s}}}\right)^n\right| + \frac{\mathrm{e}^{-I_{\max}}}{2}\sum_{n=P_{\mathrm{cut}}+1}^{\infty}\frac{I^n_{\max}}{n!},$$
$$\times\left|1 - \mathrm{e}^{I_{\max}(1-\gamma_{\mathrm{w}}/\gamma_{\mathrm{s}})}\left(\frac{\gamma_{\mathrm{w}}}{\gamma_{\mathrm{s}}}\right)^n\right| \leqslant \frac{\mathrm{e}^{-I_{\max}}}{2}\sum_{n=0}^{P_{\mathrm{cut}}}\frac{I^n_{\max}}{n!}$$
$$\times\left|1 - \mathrm{e}^{I_{\max}(1-\gamma_{\mathrm{w}}/\gamma_{\mathrm{s}})}\left(\frac{\gamma_{\mathrm{w}}}{\gamma_{\mathrm{s}}}\right)^n\right| + \frac{\mathrm{e}^{-I_{\max}}}{2}\sum_{n=P_{\mathrm{cut}}+1}^{\infty}\frac{I^n_{\max}}{n!}. \tag{D.15}$$

In the inequality condition we have used the fact that

$$\left|1 - \mathrm{e}^{I_{\max}(1-\gamma_{\mathrm{w}}/\gamma_{\mathrm{s}})}\left(\frac{\gamma_{\mathrm{w}}}{\gamma_{\mathrm{s}}}\right)^n\right| \leqslant 1 \tag{D.16}$$

for all $n \geqslant 0$ and $I_{\max} \leqslant \log 2$ given that $\gamma_{\mathrm{s}} \geqslant \gamma_{\mathrm{v}} \geqslant \gamma_{\mathrm{w}}$. This is so because $\mathrm{e}^{I_{\max}} \geqslant \mathrm{e}^{I_{\max}(1-\gamma_{\mathrm{w}}/\gamma_{\mathrm{s}})}\left(\frac{\gamma_{\mathrm{w}}}{\gamma_{\mathrm{s}}}\right)^n \geqslant 0$. Finally, by substituting the term $\mathrm{e}^{-I_{\max}}/2\sum_{n=P_{\mathrm{cut}}+1}^{\infty} I^n_{\max}/n!$ with $1/2[1 - \mathrm{e}^{-I_{\max}}\sum_{n=0}^{P_{\mathrm{cut}}} I^n_{\max}/n!]$ we obtain equation (D.13). The derivation of the upper bound for $D_{\mathrm{v,w}}$ is analogous.

The parameters $D_{n,j,k,l}$ are given by

$$D_{n,j,k,l} = \frac{1}{2}\sum_{n=0}^{\infty}\left| e^{-\beta_{\gamma_j}^2}\frac{\beta_{\gamma_j}^{2n}}{n!} - q_{nkl}e^{-\beta_{\gamma_k}^2}\frac{\beta_{\gamma_k}^{2n}}{n!} - (1-q_{nkl})e^{-\beta_{\gamma_l}^2}\frac{\beta_{\gamma_l}^{2n}}{n!}\right|. \tag{D.17}$$

If we substitute the intensities $\beta_{\gamma_j}^2$ with the values given in equation (31) we have, therefore, that

$$\begin{aligned}
D_{n,\mathrm{s,v,w}} &= \frac{1}{2}\sum_{n=0}^{\infty}e^{-I_{\max}}\frac{I_{\max}^n}{n!}\left| 1 - q_{n\mathrm{vw}}e^{I_{\max}(1-\gamma_\mathrm{v}/\gamma_\mathrm{s})}\left(\frac{\gamma_\mathrm{v}}{\gamma_\mathrm{s}}\right)^n\right.\\
&\quad\left. - (1-q_{n\mathrm{vw}})e^{I_{\max}(1-\gamma_\mathrm{w}/\gamma_\mathrm{s})}\left(\frac{\gamma_\mathrm{w}}{\gamma_\mathrm{s}}\right)^n\right|,\\
D_{n,\mathrm{v,s,w}} &= \frac{1}{2}\sum_{n=0}^{\infty}e^{-I_{\max}}\frac{I_{\max}^n}{n!}\left| e^{I_{\max}(1-\gamma_\mathrm{v}/\gamma_\mathrm{s})}\left(\frac{\gamma_\mathrm{v}}{\gamma_\mathrm{s}}\right)^n - q_{n\mathrm{sw}}\right.\\
&\quad\left. - (1-q_{n\mathrm{sw}})e^{I_{\max}(1-\gamma_\mathrm{w}/\gamma_\mathrm{s})}\left(\frac{\gamma_\mathrm{w}}{\gamma_\mathrm{s}}\right)^n\right|,\\
D_{n,\mathrm{w,s,v}} &= \frac{1}{2}\sum_{n=0}^{\infty}e^{-I_{\max}}\frac{I_{\max}^n}{n!}\left| e^{I_{\max}(1-\gamma_\mathrm{w}/\gamma_\mathrm{s})}\left(\frac{\gamma_\mathrm{w}}{\gamma_\mathrm{s}}\right)^n - q_{n\mathrm{sv}}\right.\\
&\quad\left. - (1-q_{n\mathrm{sv}})e^{I_{\max}(1-\gamma_\mathrm{v}/\gamma_\mathrm{s})}\left(\frac{\gamma_\mathrm{v}}{\gamma_\mathrm{s}}\right)^n\right|.
\end{aligned} \tag{D.18}$$

Again, these equations involve an infinite number of terms. However, as above, it can be shown that when $I_{\max} \leqslant \log 2$ and $\gamma_\mathrm{s} \geqslant \gamma_\mathrm{v} \geqslant \gamma_\mathrm{w}$ the parameters $D_{n,\mathrm{s,v,w}}$, $D_{n,\mathrm{v,s,w}}$ and $D_{n,\mathrm{w,s,v}}$ are upper bounded by

$$\begin{aligned}
D_{n,\mathrm{s,v,w}} &\leqslant \frac{1}{2}\left\{1 - \sum_{n=0}^{P_{\mathrm{cut}}}e^{-I_{\max}}\frac{I_{\max}^n}{n!}\left(1 - \left|1 - q_{n\mathrm{vw}}e^{I_{\max}(1-\gamma_\mathrm{v}/\gamma_\mathrm{s})}\right.\right.\right.\\
&\quad\left.\left.\left.\times\left(\frac{\gamma_\mathrm{v}}{\gamma_\mathrm{s}}\right)^n - (1-q_{n\mathrm{vw}})e^{I_{\max}(1-\gamma_\mathrm{w}/\gamma_\mathrm{s})}\left(\frac{\gamma_\mathrm{w}}{\gamma_\mathrm{s}}\right)^n\right|\right)\right\},\\
D_{n,\mathrm{v,s,w}} &\leqslant \frac{1}{2}\left\{q_{n\mathrm{sw}} + (1-q_{n\mathrm{sw}})e^{I_{\max}} - \sum_{n=0}^{P_{\mathrm{cut}}}e^{-I_{\max}}\frac{I_{\max}^n}{n!}\left(q_{n\mathrm{sw}} + (1-q_{n\mathrm{sw}})\right.\right.\\
&\quad\times e^{I_{\max}} - \left|e^{I_{\max}(1-\gamma_\mathrm{v}/\gamma_\mathrm{s})}\left(\frac{\gamma_\mathrm{v}}{\gamma_\mathrm{s}}\right)^n - q_{n\mathrm{sw}} - (1-q_{n\mathrm{sw}})e^{I_{\max}(1-\gamma_\mathrm{w}/\gamma_\mathrm{s})}\right.\\
&\quad\left.\left.\left.\times\left(\frac{\gamma_\mathrm{w}}{\gamma_\mathrm{s}}\right)^n\right|\right)\right\},\\
D_{n,\mathrm{w,s,v}} &\leqslant \frac{1}{2}\left\{q_{n\mathrm{sv}} + (1-q_{n\mathrm{sv}})e^{I_{\max}} - \sum_{n=0}^{P_{\mathrm{cut}}}e^{-I_{\max}}\frac{I_{\max}^n}{n!}\left(q_{n\mathrm{sv}} + (1-q_{n\mathrm{sv}})\right.\right.\\
&\quad\times e^{I_{\max}} - \left|e^{I_{\max}(1-\gamma_\mathrm{w}/\gamma_\mathrm{s})}\left(\frac{\gamma_\mathrm{w}}{\gamma_\mathrm{s}}\right)^n - q_{n\mathrm{sv}} - (1-q_{n\mathrm{sv}})e^{I_{\max}(1-\gamma_\mathrm{v}/\gamma_\mathrm{s})}\right.\\
&\quad\left.\left.\left.\times\left(\frac{\gamma_\mathrm{v}}{\gamma_\mathrm{s}}\right)^n\right|\right)\right\},
\end{aligned} \tag{D.19}$$

for any $P_{\mathrm{cut}} \geqslant 1$. To see this, the procedure is analogous to the one used to derive equation (D.14). In particular, let us consider the quantity $D_{n,\mathrm{s,v,w}}$. From equation (D.18) we have that $D_{n,\mathrm{s,v,w}}$ can be upper bounded as

$$\begin{aligned}
D_{n,\mathrm{s,v,w}} &\leqslant \frac{1}{2}\sum_{n=0}^{P_{\mathrm{cut}}}e^{-I_{\max}}\frac{I_{\max}^n}{n!}\left| 1 - q_{n\mathrm{vw}}e^{I_{\max}(1-\gamma_\mathrm{v}/\gamma_\mathrm{s})}\left(\frac{\gamma_\mathrm{v}}{\gamma_\mathrm{s}}\right)^n\right.\\
&\quad\left. - (1-q_{n\mathrm{vw}})e^{I_{\max}(1-\gamma_\mathrm{w}/\gamma_\mathrm{s})}\left(\frac{\gamma_\mathrm{w}}{\gamma_\mathrm{s}}\right)^n\right| + \frac{1}{2}\sum_{n=P_{\mathrm{cut}}+1}^{\infty}e^{-I_{\max}}\frac{I_{\max}^n}{n!}.
\end{aligned} \tag{D.20}$$

Here we have used the fact that

$$\left| 1 - q_{n\mathrm{vw}} \mathrm{e}^{I_{\max}(1-\gamma_\mathrm{v}/\gamma_\mathrm{s})} \left(\frac{\gamma_\mathrm{v}}{\gamma_\mathrm{s}}\right)^n - (1 - q_{n\mathrm{vw}}) \mathrm{e}^{I_{\max}(1-\gamma_\mathrm{w}/\gamma_\mathrm{s})} \left(\frac{\gamma_\mathrm{w}}{\gamma_\mathrm{s}}\right)^n \right| \leqslant 1, \tag{D.21}$$

for all $n \geqslant 0$ and $I_{\max} \leqslant \log 2$ given that $\gamma_\mathrm{s} \geqslant \gamma_\mathrm{v} \geqslant \gamma_\mathrm{w}$. Equation (D.21) holds because $\mathrm{e}^{I_{\max}} \geqslant \mathrm{e}^{I_{\max}(1-\gamma_k/\gamma_s)}(\gamma_k/\gamma_s)^n \geqslant 0$ for all $k \in \{\mathrm{v}, \mathrm{w}\}$. Finally, by replacing in equation (D.20) $\mathrm{e}^{-I_{\max}}/2\sum_{n=P_{\mathrm{cut}}+1}^{\infty} I_{\max}^n/n!$ with $1/2[1 - \sum_{n=0}^{P_{\mathrm{cut}}} \mathrm{e}^{-I_{\max}} I_{\max}^n/n!]$ one obtains equation (D.19). The upper bounds for $D_{n,\mathrm{v,s,w}}$ and $D_{n,\mathrm{w,s,v}}$ can be obtained in a similar manner.

Appendix E. Toolbox for Alice and Bob, and channel model

In this appendix we introduce a simple mathematical model to characterise Alice's and Bob's devices, together with the behaviour of a typical quantum channel. This model is used to simulate the observed experimental data Q^{γ_j} and E^{γ_j}, with $j \in \{\mathrm{s}, \mathrm{v}, \mathrm{w}\}$, which is needed to evaluate the examples considered in section 4. Here we will consider that Q^{γ_j} and E^{γ_j} do not depend on the basis setting, i.e., they are equal for both the Z and the X basis.

In particular, we assume the standard decoy-state BB84 protocol with phase-encoding. In each time slot, Alice prepares two WCP, the signal and the reference pulse, whose joint phase is perfectly randomised. Then, she selects at random a phase modulation $\phi \in \{0, \pi/2, \pi, 3\pi/2\}$ and applies it to the signal pulse. The values 0 and π ($\pi/2$ and $3\pi/2$) correspond to the Z (X) basis. In addition, Alice uses an intensity modulator to randomly choose the intensity $\gamma \in \{\gamma_\mathrm{s}, \gamma_\mathrm{v}, \gamma_\mathrm{w}\}$ of both the signal and the reference pulse following the prescriptions of the decoy-state method. As a result, Alice sends Bob states of the form

$$|\Psi^{\phi,\gamma}\rangle_{\mathrm{A_p}} = \frac{1}{2\pi} \int_0^{2\pi} \hat{P}(|\sqrt{\gamma^i}\,\mathrm{e}^{\mathrm{i}\theta}\rangle_\mathrm{r} |\sqrt{\gamma^i}\,\mathrm{e}^{\mathrm{i}(\theta+\phi)}\rangle_\mathrm{s})\,\mathrm{d}\theta, \tag{E.1}$$

where the subscript s (r) identifies the signal (reference) pulse and $\theta \in [0, 2\pi)$ is a random phase.

On the receiving side, Bob uses a MZI to divide the incoming pulses into two possible paths. Then he applies a phase shift $\phi \in \{0, \pi/2\}$ together with a one-pulse delay to one of them, and he recombines both pulses at a 50:50 beamsplitter. This beamsplitter has on its ends two single-photon detectors, which we denote as D_0 and D_1. Whenever the relative phase between the two interfering pulses is 0 ($\pm\pi$) only the detector D_0 (D_1) can produce a 'click', which indicates that at least one photon has been detected. In case that both detectors 'click' Bob uses the standard post-processing step where he assigns a random value to the raw bit [67]. Given that both detectors have the same quantum efficiency and assuming for the moment that there is no side-channel in Bob's measurement unit, this data post-processing guarantees the so-called basis independent detection efficiency condition. That is, Bob's detection efficiency is the same for both BB84 bases. Each detector is described by a positive operator value measure with two elements, $\hat{F}_{\mathrm{noclick}}$ and $\hat{F}_{\mathrm{click}}$. The outcome of $\hat{F}_{\mathrm{noclick}}$ corresponds to a 'no click' event, whereas the operator $\hat{F}_{\mathrm{click}}$ gives one detection 'click'. These operators are given by

$$\begin{aligned} \hat{F}_{\mathrm{noclick}} &= (1 - p_\mathrm{d}) \sum_{n=0}^{\infty} (1 - \eta_{\mathrm{det}})^n \hat{P}(|n\rangle), \\ \hat{F}_{\mathrm{click}} &= \hat{\mathbb{1}} - \hat{F}_{\mathrm{noclick}}. \end{aligned} \tag{E.2}$$

Here p_d denotes the detector's dark count rate and η_{det} is its detection efficiency.

The quantum channel introduces loss that can be parametrised by the transmission efficiency η_{channel} given by

$$\eta_{\mathrm{channel}} = 10^{\frac{-\alpha d}{10}}, \tag{E.3}$$

where α is the loss coefficient of the channel measured in dB km^{-1} and d is the transmission distance measured in km. In addition, we assume that the QKD setup has an intrinsic error rate e_d due to misalignment and instability of the optical system.

By using the mathematical models above, it can be shown that the gain Q^{γ_j} and the error rate E^{γ_j} can be expressed as

$$\begin{aligned} Q^{\gamma_j} &= 1 - (1 - p_\mathrm{d})^2 \mathrm{e}^{-\gamma_j \eta_{\mathrm{sys}}}. \\ E^{\gamma_j} &= \frac{1}{2} + \frac{1}{2Q^{\gamma_j}} (1 - p_\mathrm{d})[\mathrm{e}^{-\gamma_j \eta_{\mathrm{sys}}(1-\mathrm{e_d})} - \mathrm{e}^{-\gamma_j \eta_{\mathrm{sys}} e_\mathrm{d}}], \end{aligned} \tag{E.4}$$

where $\eta_{\rm sys}$ represents the overall loss of the system. It is given by

$$\eta_{\rm sys} = \eta_{\rm channel}\eta_{\rm B}\eta_{\rm det}, \tag{E.5}$$

with $\eta_{\rm B}$ being the internal loss of Bob's measurement device without considering his detectors. That is, we assume that the total loss within Bob's receiver is $\eta_{\rm B}\eta_{\rm det}$.

Appendix F. Approaching the optimal THA with phase-randomised coherent states

In this appendix we consider the scenario where Eve's back-reflected light is phase-randomised (i.e., Case 3 in section 4), and we analyse an alternative strategy for Eve. More precisely, we assume that Eve sends Alice n-photon Fock states instead of coherent states. This constitutes her optimal strategy in this situation, and below we analyse how much could now the parameters $D_{j,k}$ deviate from the ones obtained in appendix D.

Let us consider here the standard model of a beamsplitter with transmissivity η_{γ_j} to characterise the loss introduced by Alice's device on Eve's input signals. Then, if Eve injects an n-photon state $|n\rangle$ into Alice's device, the state of the back-reflected light is given by

$$\sigma_{\gamma_j} = \sum_{k=0}^{\infty}\binom{n}{k}\eta_{\gamma_j}^{k}(1-\eta_{\gamma_j})^{n-k}|k\rangle\langle k|, \tag{F.1}$$

The trace distance between these states and the ones given by equation (32) is

$$d(\rho_{\gamma_j}, \sigma_{\gamma_j}) := \frac{1}{2}\sum_{k=0}^{\infty}|P_{\eta_{\gamma_j}\mu}(k) - B_{\eta_{\gamma_j}}(n, k)|, \tag{F.2}$$

where $P_{\eta_{\gamma_j}\mu}(k) := \mathrm{e}^{-\eta_{\gamma_j}\mu}(\eta_{\gamma_j}\mu)^k/k!$ is a Poisson distribution of mean $\eta_{\gamma_j}\mu$, $B_{\eta_{\gamma_j}}(n, k) := \binom{n}{k}\eta_{\gamma_j}^{k}(1-\eta_{\gamma_j})^{n-k}$ is a Binomial distribution, and η_{γ_j} denotes Alice's transmission rate. When compared to the notation used in equation (32), note that $\beta_{\gamma_j}^2 := \eta_{\gamma_j}\mu$, with μ being the intensity of Eve's input pulses. Importantly, from [68] we have that whenever $\mu = n$ (i.e., the intensity of Eve's input pulses is the same in both scenarios) then equation (F.2) can be upper bounded by

$$d(\rho_{\gamma_j}, \sigma_{\gamma_j}) \leqslant 2\eta_{\gamma_j}. \tag{F.3}$$

Then, by using the triangle inequality we have that the trace distance between σ_{γ_j} and σ_{γ_k} is upper bounded by

$$d(\sigma_{\gamma_j}, \sigma_{\gamma_k}) = \frac{1}{2}\sum_{k=0}^{\infty}|B_{\eta_{\gamma_j}}(n, k) - B_{\eta_{\gamma_k}}(n, k)| \leqslant 2(\eta_{\gamma_j} + \eta_{\gamma_k}) + D_{j,k}, \tag{F.4}$$

where $D_{j,k} = d(\rho_{\gamma_j}, \rho_{\gamma_k})$ is given by equation (D.12).

In the examples considered in section 4 the parameters η_{γ_j} are typically very small (of the order of 10^{-13}–10^{-18} for a 1 GHz-clocked QKD system) for all $j \in \{\mathrm{s}, \mathrm{v}, \mathrm{w}\}$. This means, in particular, that $d(\sigma_{\gamma_j}, \sigma_{\gamma_k}) \approx D_{j,k}$ and, therefore, the results presented in section 4 (see Case 3) are also valid for the scenario where Eve injects n-photon Fock states into Alice's device.

References

[1] Vernam G S 1926 *J. Am. Inst. Elect. Eng.* **45** 109–15
[2] Shannon C E 1949 *Bell Syst. Tech. J.* **28** 656–715
[3] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing (Bangalore, India)* (Piscataway, NJ: IEEE) pp 175–9
[4] Gisin N, Ribordy R, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145–95
[5] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dusek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301–50
[6] Lo H-K, Curty M and Tamaki K 2014 *Nat. Photon.* **8** 595–604
[7] Qi B, Fung C-H F, Lo H-K and Ma X 2007 *Quantum Inf. Comput.* **7** 73–82
[8] Lamas-Linares A and Kurtsiefer C 2007 *Opt. Express* **15** 9388–93
[9] Zhao Y, Fung C-H F, Qi B, Chen C and Lo H-K 2008 *Phys. Rev.* A **78** 042333
[10] Lydersen L *et al* 2010 *Nat. Photon.* **4** 686–9
[11] Xu F, Qi B and Lo H-K 2010 *New J. Phys.* **12** 113026
[12] Weier H *et al* 2011 *New J. Phys.* **13** 073024
[13] Gerhardt I *et al* 2011 *Nat. Commun.* **2** 349
[14] Jouguet P, Kunz-Jacques S and Diamanti E 2013 *Phys. Rev.* A **87** 062313
[15] Fung C-H F, Qi B, Tamaki K and Lo H-K 2007 *Phys. Rev.* A **75** 032314
[16] Nauerth S *et al* 2009 *New J. Phys.* **11** 065001
[17] Jiang M-S, Sun S-H, Tang G-Z, Ma X-C, Li C-Y and Liang L-M 2013 *Phys. Rev.* A **88** 062335

[18] Mayers D and Yao A C-C 1998 *Proc. 39th Annual Symp. on Foundations of Computer Science (FOCS98)* (Washington, DC: IEEE Computer Society) pp 503–9
[19] Acín A, Brunner N, Gisin N, Massar S, Pironio S and Scarani V 2007 *Phys. Rev. Lett.* **98** 230501
[20] Reichardt B W, Unger F and Vazirani U 2013 *Nature* **496** 456–60
[21] Vazirani U and Vidick T 2014 *Phys. Rev. Lett.* **113** 140501
[22] Lo H-K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[23] Hensen B *et al* 2015 *Nature* **526** 682–6
[24] Giustina M *et al* 2015 *Phys. Rev. Lett.* **115** 250401
[25] Shalm L K *et al* 2015 *Phys. Rev. Lett.* **115** 250402
[26] Gisin N, Pironio S and Sangouard N 2010 *Phys. Rev. Lett.* **105** 070501
[27] Curty M and Moroder T 2011 *Phys. Rev.* A **84** 010304(R)
[28] Tamaki K, Curty M, Kato G, Lo H-K and Azuma K 2014 *Phys. Rev.* A **90** 052314
[29] Xu F, Curty M, Qi B and Lo H-K 2015 *IEEE J. Sel. Top. Quantum Electron.* **21** 6601111
[30] Curty M *et al* 2014 *Nat. Commun.* **5** 3732
[31] Rubenok A, Slater J A, Chan P, Lucio-Martinez I and Tittel W 2013 *Phys. Rev. Lett.* **111** 130501
[32] Ferreira da Silva T, Vitoreti D, Xavier G B, do Amaral G C, Temporão G P and von der Weid J P 2013 *Phys. Rev.* A **88** 052303
[33] Liu Y *et al* 2013 *Phys. Rev. Lett.* **111** 130502
[34] Tang Z, Liao Z, Xu F, Qi B, Qian L and Lo H-K 2014 *Phys. Rev. Lett.* **112** 190503
[35] Tang Y-L *et al* 2014 *Phys. Rev. Lett.* **113** 190501
[36] Tang Y-L *et al* 2015 *IEEE J. Sel. Topics Quantum Electron.* **21** 6600407
[37] Comandar L C *et al* 2016 *Nat. Photon.* **10** 312
[38] Tang Y-L *et al* 2016 *Phys. Rev.* X **6** 011024
[39] Barrett J, Colbeck R and Kent A 2013 *Phys. Rev. Lett.* **110** 010503
[40] Gisin N, Fasel S, Kraus B, Zbinden H and Ribordy G 2006 *Phys. Rev.* A **73** 022320
[41] Jain N, Stiller B, Khan I, Makarov V, Marquardt C and Leuchs G 2015 *IEEE J. Sel. Topics Quantum Electron.* **21** 6600710
[42] Lucamarini M, Choi I, Ward M B, Dynes J F, Yuan Z L and Shields A J 2015 *Phys. Rev.* X **5** 031030
[43] Hwang W-Y 2003 *Phys. Rev. Lett.* **91** 057901
[44] Lo H-K, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[45] Wang X-B 2005 *Phys. Rev. Lett.* **94** 230503
[46] Zhao Y, Qi B, Ma X, Lo H-K and Qian L 2006 *Phys. Rev. Lett.* **96** 070502
[47] Peng C-Z *et al* 2007 *Phys. Rev. Lett.* **98** 010505
[48] Rosenberg D *et al* 2007 *Phys. Rev. Lett.* **98** 010503
[49] Schmitt-Manderbach T *et al* 2007 *Phys. Rev. Lett.* **98** 010504
[50] Yuan Z L, Sharpe A W and Shields A J 2007 *Appl. Phys. Lett.* **90** 011118
[51] Liu Y *et al* 2010 *Opt. Express* **18** 8587–94
[52] Wehner S, Curty M, Schaffner C and Lo H-K 2010 *Phys. Rev.* A **81** 052336
[53] Xu K and Lo H-K 2015 arXiv:1508.07910
[54] Ma X, Qi B, Zhao Y and Lo H-K 2005 *Phys. Rev.* A **72** 012326
[55] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)
[56] Azuma K 1967 *Tohoku Math. J.* **19** 357
[57] Aharonov D, Kitaev A and Nisan N 1998 *Proc. 30th Annual ACM Symp. on Theory of Computation (STOC) (Dallas, TX, USA)* (New York: ACM) pp 20–30
[58] Zhao Y, Qi B and Lo H-K 2008 *Phys. Rev.* A **77** 052327
[59] Zhao Y, Qi B, Lo H-K and Qian L 2010 *New J. Phys.* **12** 023024
[60] Gottesman D, Lo H-K, Lütkenhaus N and Preskill J 2004 *Quant. Inf. Comput.* **4** 325–60
[61] Lo H-K and Preskill J 2007 *Quantum Inf. Comput.* **7** 431–58
[62] Tamaki K, Koashi M and Imoto N 2003 *Phys. Rev. Lett.* **90** 167904
[63] Wood R M 2003 *Laser-Induced Damage of Optical Materials* (London: Taylor and Francis)
[64] Loudon R 1973 *The Quantum Theory of Light* (New York: Oxford University Press)
[65] Lucamarini M, Patel K A, Dynes J F, Fröhlich B, Sharpe A W, Dixon A R, Yuan Z L, Penty R V and Shields A J 2013 *Opt. Express* **21** 024550
[66] Vanderbei R J 2008 *Linear Programming: Foundations and Extensions* (*International Series in Operations Research and Management Science*) 3rd edn (Berlin: Springer)
[67] Lütkenhaus N 1999 *Appl. Phys.* B **69** 395–400
[68] LeCam L 1965 *Bernoulli 1713 Bayes 1763 Laplace 1813* (Berlin: Springer) pp 179–202